PATENT
Customer Number 22,852
Attorney Docket No. 7451.0010-01
InterTrust Ref. No.: IT-14.1 (US)

CERTIFICATE OF EXPRESS MAILING

I hereby certify that this correspondence is being deposited with the United States Postal Service's "Express Mail Post Office to Addressee" service under 37 CFR § 1.10, in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on November 21, 2003. Express Mail Label No.: EV 398888405 US

Signed: Cindy Baglietto
Cindy Baglietto

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:	
Victor H. SHEAR et al.	Group Art Unit: 3629
Serial No.: 09/498,369	Examiner: T.A. DIXON
Filed: February 4, 2000	
For: METHODS FOR MATCHING, SELECTING, NARROWCASTING, AND/OR CLASSIFYING BASED ON RIGHTS MANAGEMENT AND/OR OTHER INFORMATION	

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

SECOND UPDATED NOTICE REGARDING RELATED LITIGATION

Further to the submission of the Updated Notice Regarding Related Litigation on April 14, 2003, Applicants submit this Second Updated Notice to inform the Examiner of the status of the ongoing litigation between InterTrust and Microsoft, captioned InterTrust Tech. Corp. v. Microsoft Corp. (C 01-1640 SBA, N. D. Ca.). Applicants also submit copies of papers exchanged by the parties in the course of this litigation. Many of these papers relate to claim construction.

FINNEGAN
HENDERSON
FARABOW
GARRETT &
DUNNER LLP

1300 I Street, NW
Washington, DC 20005
202.408.4000
Fax 202.408.4400
www.finnegan.com

STATUS OF RELATED LITIGATION

On March 14, 2003, the parties filed a revised Joint Claim Construction and Prehearing Statement, which includes Exhibits A-I. *See* Exhibit 1.

On April 7, 2003, InterTrust filed a Memorandum of Points and Authorities of Plaintiff InterTrust Technologies in Opposition to Microsoft Motion for Summary Judgment on Indefiniteness and Cross-Motion for Summary Judgment. *See* Exhibit 2. Also on April 7, 2003, Microsoft filed its Markman Brief. *See* Exhibit 3.

On April 21, 2003, InterTrust filed its Reply Memorandum on Claim Construction. *See* Exhibit 4. On April 21, 2003, Microsoft filed a Reply to InterTrust's Opposition to Microsoft's Brief in Support of Motion for Summary Judgment That Certain "Mini-*Markman*" Claims are Invalid for Indefiniteness. *See* Exhibit 5.

On July 3, 2003, Judge Saundra Brown Armstrong issued an Order Denying Motion for Partial Summary Judgment and Construing "Mini-*Markman* Claims. *See* Exhibit 6.

REMARKS

Applicants submit this Second Updated Notice Regarding Related Litigation, as well as the previous two Notices Regarding Related Litigation, in fulfillment of their duty to disclose information material to patentability under 37 CFR 1.56.

Applicants encourage the Examiner to read the attached documents, particularly the Court's Order dated July 3, 2003 ("Markman Order"). Applicants wish to point out that, in the Markman Order, Judge Armstrong <u>denied</u> Microsoft's Motion for Summary Judgment, also referred to in the Markman Order as the "Indefiniteness Motion." Ex. 6 at 1. Microsoft had argued that InterTrust claims that use the terms "secure," "protected

FINNEGAN
HENDERSON
FARABOW
GARRETT &
DUNNER LLP

1300 I Street, NW
Washington, DC 20005
202.408.4000
Fax 202.408.4400
www.finnegan.com

processing environment," or "host processing environment" were invalid as indefinite. Id. at 4-5. The Court rejected this argument.

The Court also construed several terms and phrases at issue in the litigation, including: (1) aspect; (2) authentication; (3) clearinghouse; (4) compares; (5) derive; (6) designating; (7) device class; (8) digital signature / digital signing; (9) digitally signing a second load module with a second digital signature different from the first digital signature, the second digital signature designating the second load module for use by a second device class having at least one of tamper resistance and security level different from the at least one of tamper resistance and security level of the first device class; (10) executable programming / executable; (11) identifying at least one aspect of an execution space required for use and/or execution of the load module; (12) Virtual Distribution Environment (VDE); (13) budget; (14) a budget specifying the number of copies which can be made of said digital file; (15) component assembly; (16) contain; (17) control; (18) controlling; (19) controlling the copies made of said digital file; (20) copy, copied, copying; (21) derives information from one or more aspects of said host processing environment; (22) Host Processing Environment (HPE); (23) identifier; (24) Protected Processing Environment (PPE); (25) secure, securely; (26) secure container; (27) securely applying, at said first appliance through use of said at least one resource said first entity's control and said second entity's control to govern use of said data item; (28) tamper resistance; (29) tamper resistant barrier; and (30) use. For the Court's construction of these terms, the Examiner is directed to pages 21-55 of the Markman Order. Applicants wish to point out that with regard to most, if not all, construed claim

FINNEGAN
HENDERSON
FARABOW
GARRETT &
DUNNER LLP

1300 I Street, NW
Washington, DC 20005
202.408.4000
Fax 202.408.4400
www.finnegan.com

terms, the Court adopted constructions substantially similar to those proposed by InterTrust.

With this Notice, Applicants have provided copies of some of the exhibits referred to in the provided papers. However, due to the voluminous number of documents referred to by these and previously provided papers, all attachments and exhibits have not been provided. If the Examiner believes a reference or a document not yet submitted may be helpful in resolving an issue before him and would like to review that or any other document, Applicants invite the Examiner to contact the undersigned at (650) 849-6621.

If there are any fees due with the filing of this Notice which have not yet been paid, please charge the fees to our Deposit Account No. 06-0916.

Respectfully submitted,

FINNEGAN, HENDERSON, FARABOW,
GARRETT & DUNNER, L.L.P.

Dated: November 21, 2003

By: Linda J. Thayer
Reg. No. 45,681

FINNEGAN
HENDERSON
FARABOW
GARRETT &
DUNNER LLP

1300 I Street, NW
Washington, DC 20005
202.408.4000
Fax 202.408.4400
www.finnegan.com

WILLIAM L. ANTHONY (State Bar No. 106908)
ERIC L. WESENBERG (State Bar No. 139696)
MARK R. WEINSTEIN (State Bar No. 193043)
ORRICK, HERRINGTON & SUTCLIFFE, LLP
1000 Marsh Road
Menlo Park, CA 94025
Telephone: (650) 614-7400
Facsimile: (650) 614-7401

JOHN W. KEKER (State Bar No. 49092)
MICHAEL H. PAGE (State Bar No. 154913)
KEKER & VAN NEST, LLP
710 Sansome Street
San Francisco, CA 94111-1704
Telephone: (415) 391-5400
Facsimile: (415) 397-7188

Additional Counsel Listed at Signature Block

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

OAKLAND DIVISION

INTERTRUST TECHNOLOGIES CORPORATION, a Delaware corporation,

Plaintiff,

v.

MICROSOFT CORPORATION, a Washington corporation,

Defendant.

MICROSOFT CORPORATION, a Washington corporation,

Counterclaimant,

v.

INTERTRUST TECHNOLOGIES CORPORATION, a Delaware corporation,

Counter Claim-Defendant.

Case No. C 01-1640 SBA (MJE)

PATENT LOCAL RULE 4-3 JOINT CLAIM CONSTRUCTION AND PREHEARING STATEMENT REVISED IN ACCORDANCE WITH THE SCOPE OF "MINI-*MARKMAN*" HEARING SET FORTH IN THE COURT'S ORDER ENTERED 2/24/03

In accordance with the Court's Order entered February 24, 2003 and Patent Local Rule 4-3, Plaintiff and Counter-Defendant InterTrust Technologies ("InterTrust") and Defendant and Counter-Claimant Microsoft Corporation ("Microsoft") submit the following revised Joint Claim Construction and Prehearing Statement. Pursuant to that Order, the parties have limited their disputes for purposes of the "Mini-*Markman*" proceeding, to 30 disputed terms and phrases, as identified in alphabetical order in Exhibit B and highlighted in copies of the claims in Exhibit H, hereto.

Submission of "Intrinsic" Evidence

To avoid unnecessary duplication, the parties will submit, prior to the submission of the final briefs in the "Mini-*Markman*" proceeding (including briefing addressing indefiniteness), a Joint Declaration presenting the Intrinsic evidence (including patents, file histories and cited references). The parties agree that in briefs submitted in the "Mini-*Markman*" proceeding, a party may cite to evidence that ultimately will be submitted by the parties in such Joint Declaration and need not append such evidence to a declaration in support of a brief. This agreement does not limit either party from submitting any evidence with a declaration accompanying any brief.

RULE 4-3(a): Agreed Construction

- Attached hereto as **Exhibit I** is a list of claim constructions upon which the parties agree. To the extent that agreed constructions refer to disputed terms that are not among the 30 terms in the "Mini-*Markman*" proceeding, such terms are set forth in quotations.

RULE 4-3(b): Disputed Claim Construction Presentation

- Attached hereto as **Exhibit A** is a list of disputed claim terms set forth in claim order, together with the parties' proposed constructions.
- Attached hereto as **Exhibit B** is a list of the 30 disputed claim terms in alphabetical order, together with the parties' proposed constructions.
- Attached hereto as **Exhibit C** is InterTrust's identification of intrinsic and extrinsic evidence supporting its proposed construction for each of the 30 disputed terms and phrases.

- Attached hereto as **Exhibit D** is Microsoft's identification of intrinsic and extrinsic evidence supporting its proposed construction for each of the 30 disputed terms and phrases.
- Attached hereto as **Exhibit E** is a Microsoft statement of reservations.
- Attached hereto as **Exhibit H** is the text of the 12 claims at issue, with bolding identifying the terms and phrases in dispute for the purposes of the "Mini-*Markman*" proceeding.

RULE 4-3(c): Claim Construction Hearing Length

The claim construction schedule is set forth in the Court's Order entered February 24, 2003.

RULE 4-3(d): Witness Testimony

The parties have agreed to present witness testimony through declarations filed in support of the briefs. There also shall be tutorial presentations, per the Court's Order of February 24, 2003.

- Attached hereto as **Exhibit F** is a summary of expert testimony to be presented by InterTrust.
- Attached hereto as **Exhibit G** is a summary of expert testimony to be presented by Microsoft.

RULE 4-3(e): Pre-Hearing Conference Issues

The parties addressed pre-hearing matters at the Case Management Conference hearing on February 13, 2003. No pre-hearing conference is currently scheduled or requested.

Dated: March 14, 2003

INTERTRUST TECHNOLOGIES CORPORATION
MARK SCADINA - #173103
JEFF MCDOW - #184727
4800 Patrick Henry Drive
Santa Clara, CA 95054
Telephone: (408) 855-0100
Facsimile: (408) 855-0144

By: FOR JEFF McDOW
Jeff McDow

KEKER & VAN NEST, LLP
MICHAEL H. PAGE

DERWIN & SIEGEL
DOUGLAS K. DERWIN - #111407
3280 Alpine Road
Portola Valley, CA 94028
Telephone: (650) 529-8700
Facsimile: (650) 529-8799

Attorneys for Plaintiff and Counter-Defendant
INTERTRUST TECHNOLOGIES
CORPORATION

Dated: March 14, 2003

WILLIAM L. ANTHONY
HEIDI L. KEEFE
MARK R. WEINSTEIN
ORRICK, HERRINGTON & SUTCLIFFE LLP

By: ______________________
Sam O'Rourke

KLARQUIST SPARKMAN, LLP
One World Trade Center
121 S.W. Salmon, Suite 1600
Portland, OR 97204
Telephone: (503) 226-7391
Facsimile: (503) 228-9446

Attorneys for Microsoft Corporation

EXHIBIT A

Intertrust v. MS: JCCS Claim Chart

U.S. Patent No. 6,253,193, Asserted Claim 1

	'193 Claim 1	IT Construction	MS Construction
1.	1. A method comprising:	The claim contains no requirement of a VDE.	Claim as a whole: The recited method is performed within a **VDE**. (See item #86 for Microsoft's construction of **VDE**.)
2.	receiving a digital file including music,		
3.	storing said digital file in a first **secure** memory of a first device;	secure: One or more mechanisms are employed to prevent, detect or discourage misuse of or interference with information or processes. Such mechanisms may include concealment, Tamper Resistance, Authentication and access control. Concealment means that it is difficult to read information (for example, programs may be encrypted). Tamper Resistance and Authentication are separately defined (see item #67 and item #27, respectively, below). Access control means that access to information or processes is limited on the basis of authorization. Security is not absolute, but is designed to be sufficient for a particular purpose.	secure: (1) A state in which all users of a system are guaranteed that all information, processes, and devices within the system, shall have their availability, secrecy, integrity, authenticity and nonrepudiation maintained against all of the identified threats thereto. (2) "Availability" means the property that information is accessible and usable upon demand by authorized persons, at least to the extent that no user may delete the information without authorization. (3) "Secrecy," also referred to as confidentiality, means the property that information (including computer processes) is not made available or disclosed to unauthorized persons or processes. (4) "Integrity" means the property that information has not been altered either intentionally or accidentally. (5) "Authenticity" means the property that the characteristics asserted about a person, device, program, information, or process are genuine and timely, particularly as to identity, data integrity, and origin integrity. (6) "Nonrepudiation" means the property that a sender of information cannot deny its origination and that a recipient of information cannot deny its receipt.

	'193 Claim 1	IT Construction	MS Construction
4.	storing information associated with said digital file in a **secure** database stored on said first device, said information including at least one **budget control** and	secure: see item #3 above budget: Information specifying a limitation on usage. control: Information and/or programming controlling operations on or use of resources (e.g., content) including (a) permitted, required or prevented operations, (b) the nature or extent of such operations or (c) the consequences of such operations.	secure: see item #3 above budget: (1) A unique type of "method" that specifies a decrementable numerical limitation on future **Use** (e.g., copying) of digital information and how such **Use** will be paid for, if at all. (2) A "method" is a collection of basic instructions, and information related to basic instructions, that provides context, data, requirements, and/or relationships for use in performing, and/or preparing to perform, basic instructions in relation to the operation of one or more electronic appliances. control: (1) Independent, special-purpose, **Executable**, which can execute only within a *Secure Processing Environment* (see below). (2) Each **VDE Control** is a **Component Assembly** dedicated to a particular activity (e.g., editing, modifying another **Control**, a user-defined action, etc.), particular user(s), and particular protected information, and whose satisfactory execution is necessary to *Allowing* (see below) that activity. (3) Each separate information *Access* (see below) or **Use** is independently **Controlled** by independent **VDE Control(s)**. (4) Each **VDE Control** is assembled within a *Secure Processing Environment* from independently deliverable modular components (e.g., *Load Modules* (see below) or other **Controls**), dynamically in response to an information *Access* or **Use** Request. (5) The dynamic assembly of a **Control** is directed by a "blueprint" *Record* (see below) (put in place by one or more **VDE** users) **Containing** control information identifying the exact modular code components to be

	'193 Claim 1	IT Construction	MS Construction
			assembled and executed to govern (i.e., **Control**) this particular activity on this particular information by this particular user(s). (6) Each **Control** is independently assembled, loaded and delivered vis-à-vis other **Controls**. (7) Control information and **Controls** are extensible and can be configured and modified by all users, and combined by all users with any other **VDE** control information or **Controls** (including that provided by other users), subject only to "senior" user **Controls**. (8) Users can assign control information (including alternative control information) and **Controls** to an arbitrarily fine, user-defined portion of the protected information, such as a single paragraph of a document, as opposed to being limited to file-based controls. (9) **VDE Controls** reliably limit **Use** of the protected information to only authorized activities and amounts. For the purposes of the construction of "Control," a "*Secure Processing Environment*" is defined as: A Secure Processing Environment is uniquely identifiable, self-contained, non-circumventable, and trusted by all other **VDE** nodes to protect the availability, secrecy, integrity and authenticity of all information identified in the patent application as being protected, and to guarantee that such information will be accessed and **Used** only as expressly authorized by the associated **VDE Controls**, and to guarantee that all requested reporting of and payments for protected information use will be made. A Secure Processing Environment is formed by, and requires, a Secure Processing Unit having a hardware **Tamper Resistant Barrier** encapsulating a processor and internal

	'193 Claim 1	IT Construction	MS Construction
			Secure memory. The **Tamper Resistant Barrier** prevents all unauthorized interference, removal, observation, and other **Use** of the information and processes within it. For the purposes of the construction of "Control," "*Allowing*" is defined as: Actively permitting an action that otherwise cannot be taken (i.e., is prohibited) by any user, process, or device. In **VDE**, an action is allowed only through execution (within a *Secure Processing Environment*) of the **VDE Control(s)** assigned to the particular action request, and satisfaction of all requirements imposed by such execution. For the purposes of the construction of "Control," "*Access*" is defined as: To satisfactorily perform the steps necessary to obtain something so that it can be **Used** in some manner (e.g., for information: copied, printed, decrypted, encrypted, saved, modified, observed, or moved, etc.). In **VDE**, access to protected information is achieved only through execution (within a *Secure Processing Environment*) of the **VDE Control(s)** assigned to the particular "access" request, satisfaction of all requirements imposed by such execution, and the **Controlled** opening of the **Secure Container Containing** the information. For the purposes of the construction of "Control," a "*Load Module*" is defined as: An **Executable**, modular unit of machine code (which may include data) suitable for loading into memory for execution by a processor. A load module is encrypted (when not within a secure processing unit) and has an **Identifier** that a calling process must provide to be able to use the load module. A load module is combinable with other load modules,

	'193 Claim 1	IT Construction	MS Construction
			and associated data, to form **Executable Component Assemblies.** A load module can execute only in a **VDE Protected Processing Environment.** Library routines are not load modules and dynamic link libraries are not load modules. For the purposes of the construction of "Control," a "*Record*" is defined as: A data structure that is a collection of fields (elements), each with its own name and type. Unlike an array, whose elements are accessed using an index, the elements of a record are accessed by name. A record can be accessed as a collective unit of elements, or the elements can be accessed individually.
5.	at least one **copy control,**	<u>copy</u>: To reproduce. The reproduction must be usable, may incorporate all of the original item or only some of it, and may involve some changes to the item as long as the essential nature of the content remains unchanged. <u>control</u>: see item #4 above	<u>copy</u>: (1) To reproduce all of a *Digital File* (see below) or other complete physical block of data from one location on a storage medium to another location on the same or different storage medium, leaving the original block of data unchanged, such that two distinct and independent objects exist. (2) Although the layout of the data values in physical storage may differ from the original, the resulting "copy" is logically indistinguishable from the original. (3) The resulting "copy" may or may not be encrypted, ephemeral, usable, or accessible. For the purposes of the construction of "Copy," a "*Digital File*" is defined as: A named, static unit of storage allocated by a "file system" and **Containing** digital information. A digital file enables any application using the "file system" to randomly access its contents and to distinguish it by name from every other such unit. A copy of a digital file is a separate digital file. A "file system" is the portion of the operating system

	'193 Claim 1	IT Construction	MS Construction
			that translates requests made by application programs for operations on "files" into low-level tasks that can control storage devices such as disk drives. control: see item #4 above
6.	said at least one **budget control** including ***a budget*** *specifying the number of copies which can be made of said digital file*;	budget: see item #4 above control: see item #4 above a budget specifying the number of copies which can be made of said digital file: Normal English, incorporating the separately defined terms: a Budget stating the number of copies that can be made of the digital file referred to earlier in the claim.	budget: see item #4 above control: see item #4 above a budget specifying the number of copies which can be made of said digital file: A **Budget** explicitly stating the total number of copies (whether or not decrypted, long-lived, or accessible) that (since creation of the **Budget**) are authorized to be made of the *Digital File* by any and all users, devices, and processes. No process, user, or device is able to make another copy of the *Digital File* once this number of copies has been made. For the purposes of the construction of this phrase, "*Digital File*" is defined as set forth in item #5, above.
7.	and said at least one **copy control** *controlling the copies made of said digital file*;	copy: see item #5 above control: see item #4 above controlling: Normal English: exercising authoritative or dominating influence over; directing. controlling the copies made of said digital file: The nature of this operation is further defined in later claim elements. In context, the copy control determines the conditions under which a digital file may be Copied and the copied file stored on a second device.	copy: see item #5 above control: see item #4 above controlling: (1) Reliably defining and enforcing the conditions and requirements under which an action that otherwise cannot be taken, will be *Allowed*, and the manner in which it may occur. Absent verified satisfaction of those conditions and requirements, the action cannot be taken by any user, process or device. (2) In **VDE**, an action is **Controlled** through execution of the applicable **VDE Control(s)** within a **VDE** *Secure Processing Environment*. (3) More specifically, in **VDE**, **Controlling** is effected by use of **VDE Controls**, **VDE Secure Containers**, and **VDE** foundation

	'193 Claim 1	IT Construction	MS Construction
			(including **VDE** *Secure Processing Environment*, "object registration," and other mechanisms for allegedly individually ensuring that specific **Controls** are enforced vis-à-vis specific objects (and their content at an arbitrary granular level) and specific "users"). For the purposes of the construction of "Control (v.)" et al, "*Allowed*" and "*Secure Processing Environment*" are defined as set forth in item #4, above. <u>controlling the copies made of said digital file</u>: **Controlling Uses** of and *Accesses* to all copies of the *Digital File*, by all users, processes, and devices, by executing each of the recited "at least one" **Copy Control(s)** within **VDE** *Secure Processing Environment(s).* Each **Control** governs **(Controls)** only one action, which action may or may not differ among the different "at least one" **Controls**. All **Uses** and *Accesses* are prohibited and incapable of occurring except to the extent *Allowed* by the "at least one" **Copy Control(s)**. For the purposes of the construction of this phrase, "*Secure Processing Environment,*" "*Access*" and "*Allowed*" are defined as set forth in item #4, above.

	'193 Claim 1	IT Construction	MS Construction
8.	determining whether said digital file may be **copied** and stored on a second device based on at least said **copy control**;	copied (copy): see item #5 above control: see item #4 above	copied (copy): see item #5 above control: see item #4 above
9.	if said **copy control** allows at least a portion of said digital file to be **copied** and stored on a second device,	copied (copy): see item #5 above control: see item #4 above	copied (copy): see item #5 above control: see item #4 above
10.	**copying** at least a portion of said digital file;	copying (copy): see item #5 above	copying (copy): see item #5 above
11.	transferring at least a portion of said digital file to a second device including a memory and an audio and/or video output;		
12.	storing said digital file in said memory of said second device; and		
13.	including playing said music through said audio output.		

U.S. Patent No. 6,253,193, Asserted Claim 11

	'193 Claim 11	IT Construction	MS Construction
14.	11. A method comprising:	The claim contains no requirement of a VDE.	Claim as a whole: The recited method is performed within a **VDE**. (See item #86 for Microsoft's construction of **VDE**.)
15.	receiving a digital file;		
16.	storing said digital file in a first **secure** memory of a first device;	secure: see item #3 above	secure: see item #3 above
17.	storing information associated with said digital file in a **secure** database stored on said first device, said information including a first **control**;	secure: see item #3 above control: see item #4 above	secure: see item #3 above control: see item #4 above
18.	determining whether said digital file may be **copied** and stored on a second device based on said first **control**, said determining step including identifying said second device and determining whether,	copied (copy): see item #5 above control: see item #4 above	copied (copy): see item #5 above control: see item #4 above
19.	said first **control** allows transfer of said **copied** file to said second device, said determination based at least in part on the features present at the device to which said **copied** file is to be transferred;	control: see item #4 above copied (copy): see item #5 above	control: see item #4 above copied (copy): see item #5 above

	'193 Claim 11	IT Construction	MS Construction
20.	if said first **control** allows at least a portion of said digital file to be **copied** and stored on a second device,	control: see item #4 above copied (copy): see item #5 above	control: see item #4 above copied (copy): see item #5 above
21.	**copying** at least a portion of said digital file;	copying (copy): see item #5 above	copying (copy): see item #5 above
22.	transferring at least a portion of said digital file to a second device including a memory and an audio and/or video output;		
23.	storing said digital file in said memory of said second device; and		
24.	rendering said digital file through said output.		

U.S. Patent No. 6,253,193, Asserted Claim 15

	'193 Claim 15	IT Construction	MS Construction
25.	15. A method comprising:	The claim contains no requirement of a VDE.	Claim as a whole: The recited method is performed within a **VDE**. (See item #93 for Microsoft's construction of **VDE**.)
26.	receiving a digital file;		
27.	an **authentication** step comprising:	authentication: Identifying (e.g., a person, device, organization, document, file, etc.). Includes uniquely identifying or identifying as a member of a group.	authentication: To establish that the following asserted characteristics of something (e.g., a person, device, organization, document, file, etc.) are genuine: its identity, its data integrity, (i.e., it has not been altered) and its origin integrity (i.e., its source and time of origination).
28.	accessing at least one **identifier** associated with a first device or with a user of said first device; and	identifier: Information used to identify something or someone (e.g., a password). In this definition, "identify" means to establish the identity of or to ascertain the origin, nature, or definitive characteristics of; includes identifying as an individual or as a member of a group.	identifier: Any text string used as a label naming an individual instance of what it *Identifies* (see below) For the purpose of the construction of "Identifier," *"Identify"* is defined as: To establish as being a particular instance of a person or thing.
29.	determining whether said **identifier** is associated with a device and/or user authorized to store said digital file;	identifier: see item #28 above	identifier: see item #28 above
30.	storing said digital file in a first **secure** memory of said first device, but only if said device and/or user is so authorized, but not proceeding with said storing if said device and/or user is not authorized;	secure: see item #3 above	secure: see item #3 above
31.	storing information associated with said digital file in a **secure** database stored on said first	secure: see item #3 above control: see item #4 above	secure: see item #3 above control: see item #4 above

	'193 Claim 15	IT Construction	MS Construction
	device, said information including at least one **control**;		
32.	determining whether said digital file may be **copied** and stored on a second device based on said at least one **control**;	copied (copy): see item #5 above control: see item #4 above	copied (copy): see item #5 above control: see item #4 above
33.	if said at least one **control** allows at least a portion of said digital file to be **copied** and stored on a second device,	control: see item #4 above copied (copy): see item #5 above	control: see item #4 above copied (copy): see item #5 above
34.	**copying** at least a portion of said digital file;	copying (copy): see item #5 above	copying (copy): see item #5 above
35.	transferring at least a portion of said digital file to a second device including a memory and an audio and/or video output;		
36.	storing said digital file in said memory of said second device; and		
37.	rendering said digital file through said output.		

U.S. Patent No. 6,253,193, Asserted Claim 19

	'193 Claim 19	**IT Construction**	**MS Construction**
38.	19. A method comprising:	The claim contains no requirement of a VDE.	Claim as a whole: The recited method is performed within a **VDE**. (See item #86 for Microsoft's construction of **VDE**.)
39.	receiving a digital file at a first device;		
40.	establishing communication between said first device and a **clearinghouse** located at a location remote from said first device;	clearinghouse: A provider of financial and/or administrative services for a number of entities; or an entity responsible for the collection, maintenance, and/or distribution of materials, information, licenses, etc.	clearinghouse: (1) A computer system that provides intermediate storing and forwarding services for both content and audit information, and which two or more parties trust to provide its services independently because it is operated under constraint of **VDE** security. (2) "Audit information" means all information created, stored, or reported in connection with an "auditing" process. "Auditing" means tracking, metering and reporting the usage of particular information or a particular appliance.
41.	said first device obtaining authorization information including a key from said **clearinghouse**;	clearinghouse: see item #40 above	clearinghouse: see item #40 above
42.	said first device using said authorization information to gain access to or make at least one **use** of said first digital file, including using said key to decrypt at least a portion of said first digital file; and	use: Normal English: to put into service or apply for a purpose, to employ.	use: (1) To use information is to perform some action on it or with it (e.g., copying, printing, decrypting, encrypting, saving, modifying, observing, or moving, etc.). (2) In **VDE**, information **Use** is *Allowed* only through execution of the applicable **VDE Control(s)** and satisfaction of all requirements imposed by such execution. For the purposes of the construction of "Use," "*Allowed*" is defined as set forth in item #4, above.
43.	receiving a first **control** from said **clearinghouse** at said first device;	control: see item #4 above clearinghouse: see item #40 above	control: see item #4 above clearinghouse: see item #40 above

	'193 Claim 19	IT Construction	MS Construction
44.	storing said first digital file in a memory of said first device;		
45.	using said first **control** to determine whether said first digital file may be **copied** and stored on a second device;	control: see item #4 above copied (copy): see item #5 above	control: see item #4 above copied (copy): see item #5 above
46.	if said first **control** allows at least a portion of said first digital file to be **copied** and stored on a second device,	control: see item #4 above copied (copy): see item #5 above	control: see item #4 above copied (copy): see item #5 above
47.	**copying** at least a portion of said first digital file;	copying (copy): see item #5 above	copying (copy): see item #5 above
48.	transferring at least a portion of said first digital file to a second device including a memory and an audio and/or video output;		
49.	storing said first digital file portion in said memory of said second device; and		
50.	rendering said first digital file portion through said output.		

U.S. Patent No. 6,185,683, Asserted Claim 2

	'683 Claim 2	IT Construction	MS Construction
51.	2. A system including:	The claim contains no requirement of a VDE.	Claim as a Whole: The "system" is a VDE. (See item #86 for Microsoft's construction of **VDE**.)
52.	a first apparatus including,		
53.	user **controls**,	<u>control</u>: see item #4 above	<u>control</u>: see item #4 above
54.	a communications port,		
55.	a processor,		
56.	a memory storing:		
57.	a first **secure container**	<u>secure container</u>: A container that is Secure. In this definition, "container" means a digital file containing linked and/or embedded items.	<u>secure container</u>: (1) A **VDE Secure Container** is a self-contained, self-protecting data structure which (a) encapsulates information of arbitrary size, type, format, and organization, including other, nested, containers, (b) cryptographically protects that information from all unauthorized *Access* and **Use**, (c) provides encrypted storage management functions for that information, such as hiding the physical storage location(s) of its protected contents, (d) permits the association of itself or its contents with **Controls** and control information governing (**Controlling**) *Access* to and **Use** thereof, and (e) prevents such **Use** or *Access* (as opposed to merely preventing decryption) until it is "opened." (2) A **Secure Container** can be opened only as expressly *Allowed* by the associated **VDE Control(s)**, only within a *Secure Processing Environment*, and only through decryption of its encrypted header. (3) A **Secure Container** is not directly accessible to any non-**VDE** or user calling process. All such calls are intercepted by **VDE**. (4) The creator of a **Secure Container** can assign (or allow others to assign) control information to any arbitrary portion of a **Secure Container**'s contents, or to an empty **Secure Container** (to govern

	'683 Claim 2	IT Construction	MS Construction
			(Control) the later addition of contents to the container, and *Access* to or **Use** of those contents). (5) A container is not a **Secure Container** merely because its contents are encrypted and signed. A **Secure Container** is itself **Secure**. (6) All **VDE**-protected information (including protected content, information about content usage, content-control information, **Controls**, and *Load Modules*) is encapsulated within a **Secure Container** whenever stored outside a *Secure Processing Environment* or secure database. For the purposes of the construction of "Secure Container," "*Secure Processing Environment,*" "*Load Module,*" "*Access*" and "*Allow*" are defined as set forth in item #4, above.
58.	**containing** a governed item,	containing: Normal English: having within or holding. In the context of an element contained within a data structure (e.g., a secure container), the contained element may be either directly within the container or the container may hold a reference indicating where the element may be found.	containing: Physically (directly) storing within, as opposed to addressing (i.e., referring to something by the explicitly identified location where it is stored, without directly storing it).
59.	the first **secure container** governed item being at least in part encrypted; the first **secure container** having been received from a second apparatus;	secure container: see item #57 above	secure container: see item #57 above

	'683 Claim 2	IT Construction	MS Construction
60.	a first **secure container** rule at least in part governing an **aspect** of access to or **use** of said first **secure container** governed item, the first **secure container** rule, the first **secure container** rule having been received from a third apparatus different from said second apparatus; and	secure container: see item #57 above aspect: Feature, element, property or state. use: see item #42 above	secure container: see item #57 above aspect: An aspect of an environment is a persistent element or property of that environment that can be used to distinguish it from other environments. use: see item #42 above
61.	hardware or software used for receiving and opening **secure containers**, said **secure containers** each including the capacity to **contain** a governed item, a **secure container** rule being associated with each of said **secure containers**;	secure container: see item #57 above contain (containing): see item #58 above	secure container: see item #57 above contain (containing): see item #58 above
62.	a **protected processing environment** at least in part protecting information **contained** in said **protected processing environment** from tampering by a user of said first apparatus,	protected processing environment: An environment in which processing and/or data is at least in part protected from tampering. The level of protection can vary, depending on the threat. In this definition, "environment" means capabilities available to a program running on a computer or other device or to the user of a computer or other device. Depending on the context, the environment may be in a single device (e.g., a personal computer) or may be spread among multiple	protected processing environment: (1) A uniquely identifiable, self-contained computing base trusted by all **VDE** nodes to protect the availability, secrecy, integrity and authenticity of all information identified in the February, 1995, patent application as being protected, and to guarantee that such information will be *Accessed* and Used only as expressly authorized by **VDE Controls**. (2) At most **VDE** nodes, the **Protected Processing Environment** is a *Secure Processing Environment* which is formed by, and requires, a

	'683 Claim 2	IT Construction	MS Construction
		devices (e.g., a network). contained (containing): see item #58 above	hardware **Tamper Resistant Barrier** encapsulating a special-purpose Secure Processing Unit having a processor and internal secure memory. "Encapsulated" means hidden within an object so that it is not directly accessible but rather is accessible only through the object's restrictive interface. (3) The **Tamper Resistant Barrier** prevents all unauthorized (intentional or accidental) interference, removal, observation, and use of the information and processes within it, by all parties (including all users of the device in which the **Protected Processing Environment** resides), except as expressly authorized by **VDE Controls.** (4) A **Protected Processing Environment** is under **Control** of **Controls** and control information provided by one or more parties, rather than being under **Control** of the appliance's users or programs. (5) Where a **VDE** node is an established financial **Clearinghouse**, or other such facility employing physical facility and user-identity **Authentication** security procedures trusted by all **VDE** nodes, and the **VDE** node does not *Access* or **Use VDE**-protected information, or assign **VDE** control information, then the **Protected Processing Environment** at that **VDE** node may instead be formed by a general-purpose CPU that executes all **VDE** "security" processes in protected (privileged) mode. (6) A **Protected Processing Environment** requires more than just verifying the integrity of **Digitally Signed Executable** programming prior to execution of the programming; or concealment of the program, associated data, and execution of the program code; or use of a password as its protection

	'683 Claim 2	IT Construction	MS Construction
			mechanism. For the purposes of the construction of "Protected Processing Environment," "*Secure Processing Environment*" and "*Access*" are defined as set forth in item #4, above. contained (containing): see item #58 above
63.	said **protected processing environment** including hardware or software used for applying said first **secure container** rule and a second **secure container** rule in combination to at least in part govern at least one **aspect** of access to or **use** of a governed item **contained** in a **secure container**; and	protected processing environment: see item #62 above secure container: see item #57 above aspect: see item #60 above use: see item #42 above contained (containing): see item #58 above	protected processing environment: see item #62 above secure container: see item #57 above aspect: see item #60 above use: see item #42 above contained (containing): see item #58 above
64.	hardware or software used for transmission of **secure containers** to other apparatuses or for the receipt of **secure containers** from other apparatuses.	secure container: see item #57 above	secure container: see item #57 above

	'721 Claim 1	IT Construction	MS Construction
65.	1. A security method comprising:	The claim contains no requirement of a VDE.	Claim as a whole: The recited method is performed within a **VDE**. (See item #86 for Microsoft's construction of **VDE**.)
66.	**digitally signing** a first load module with a first **digital signature designating** the first load module for **use** by a first **device class**;	digital signature: A digital value, verifiable with a key, that can be used to determine the source and/or integrity of a signed item (e.g., a file, program, etc.). Digitally signing is the process of creating a digital signature. designating: Normal English: indicating, specifying, pointing out or characterizing. use: see item #42 above device class: A group of devices which share at least one attribute.	digitally signing: (1) Creating a **Digital Signature** using a secret *Key* (see below). (2) In symmetric key cryptography, a "secret key" is a *Key* that is known only to the sender and recipient. In asymmetric key cryptography, a "secret key" is the private *Key* of a public/private key pair, in which the two keys are related uniquely by a predetermined mathematical relationship such that it is computationally infeasible to determine one from the other. For the purposes of the construction of "Digital Signing," a "*Key*" is defined as: A bit sequence used and needed by a cryptographic algorithm to encrypt a block of plain text or to decrypt a block of cipher text. A key is different from a key seed or other information from which the actual encryption and/or decryption key is constructed, **Derived**, or otherwise identified. In symmetric key cryptography, the same key is used for both encryption and decryption. In asymmetric or "public key" cryptography, two related keys are used; a block of text encrypted by one of the two keys (e.g., the "public key") can be decrypted only by the corresponding key (e.g., the "private key"). digital signature: A computationally unforgeable string of characters (e.g., bits) generated by a cryptographic operation on a block of data using some secret. The string can be generated only by an entity that knows the secret, and hence provides

	'721 Claim 1	IT Construction	MS Construction
			evidence that the entity must have generated it. designating: Designating something for a particular **Use** means specifying it for and restricting it to that **Use**. use: see item #42 above device class: The generic name for a group of device types. For example, all display stations belong to the same device class. A device class is different from a device type. A device type is composed of all devices that share a common model number or family (e.g. IBM 4331 printers).
67.	***digitally signing** a **second load module** with a second **digital signature** different from the first **digital signature**, the second **digital signature designating** the second load module **for use** by a second **device class** having at least one of **tamper resistance** and security level different from the at least one of **tamper resistance** and security level of the **first device class**;*	digital signature: see item #66 above designating: see item #66 above use: see item #42 above device class: see item #66 above tamper resistance: Making tampering more difficult and/or allowing detection of tampering. In this definition, "tampering" means using (e.g., observing or altering) in any unauthorized manner, or interfering with authorized use. digitally signing a second load module with a second digital signature different from the first digital signature, the second digital signature designating the second load module for use by a second device class having at least one of tamper resistance and security level different from the at least one of tamper resistance and security level of the first device class: Normal English, incorporating the separately defined terms: generating a Digital Signature	digital signature: see item #66 above designating: see item #66 above use: see item #42 above device class: see item #66 above tamper resistance: The ability of a **Tamper Resistant Barrier** to prevent *Access*, observation, and interference with information or processing encapsulated by the barrier. For the purposes of the construction of "Tamper Resistance," "*Tamper/Tampering*" is defined as: Using (e.g., observing or altering) in any unauthorized manner, or interfering with authorized use. For the purposes of the construction of "Tamper Resistance," "*Access*" is defined as set forth in item #4, above. digitally signing a second load module with a second digital signature different from the first digital signature, the second digital signature designating the second load module for use by a second device

	'721 Claim 1	IT Construction	MS Construction
		for the second load module, the Digital Signature Designating that the second load module is for use by a second Device Class. This element further requires that the second Device Class have a different Tamper Resistance or security level than the first Device Class.	class having at least one of tamper resistance and security level different from the at least one of tamper resistance and security level of the first device class: (1) **Digitally Signing** a different ("second") *Load Module* by using a different ("second") **Digital Signature** as the signature *Key*, which signing indicates to any and all devices in the second **Device Class** that the signor authorized and restricted this *Load Module* for **Use** by that device. (2) No **VDE** device can perform any execution of any *Load Module* without such authorization. The method ensures that the *Load Module* cannot execute in a particular **Device Class** and ensures that no device in that **Device Class** has the *Key(s)* necessary to verify the **Digital Signature**. (3) All devices in the first **Device Class** have the same persistent (not just occasional) and identified level of **Tamper Resistance** and the same persistent and identified level of security. All devices in the second **Device Class** have the same persistent and identified level of **Tamper Resistance** and same persistent and identified level of security. (4) The identified level of **Tamper Resistance** or identified level of security (or both) for the first **Device Class**, is greater than or less than the identified level of **Tamper Resistance** or identified level of security for the second **Device Class**. For the purposes of the construction of this phrase, a "*Load Module*" is defined as set forth in item #4 and "*Key*" is defined as set forth in item #66, above.

	'721 Claim 1	IT Construction	MS Construction
68.	distributing the first load module for **use** by at least one device in the first **device class**; and	use: see item #42 above device class: see item #66 above	use: see item #42 above device class: see item #66 above
69.	distributing the second load module for **use** by at least one device in the second **device class**.	use: see item #42 above device class: see item #66 above	use: see item #42 above device class: see item #66 above

U.S. Patent No. 6,157,721, Asserted Claim 34

	'721 Claim 34	IT Construction	MS Construction
70.	34. A **protected processing environment** comprising:	The claim contains no requirement of a VDE <u>protected processing environment</u>: see item #62 above "Protected processing environment" appears in the preamble of this claim. InterTrust reserves the right to assert that it should not be defined, other than as requiring the individual claim elements.	<u>Claim as a Whole</u>: The "**Protected Processing Environment**" is part of and within **VDE**. (See item #86 for Microsoft's construction of **VDE**.) <u>protected processing environment:</u> see item #62 above
71.	a first **tamper resistant barrier** having a first security level,	<u>tamper resistant barrier</u>: Hardware and/or software that provides Tamper Resistance.	<u>tamper resistant barrier</u>: (1) An active device that encapsulates and separates a **Protected Processing Environment** from the rest of the world. (2) It prevents information and processes within the **Protected Processing Environment** from being observed, interfered with, and leaving except under appropriate conditions ensuring security. (3) It also **Controls** external access to the encapsulated **Secure** resources, processes and information. (4) A **Tamper Resistant Barrier** is capable of destroying protected information in response to *Tampering* attempts. For the purposes of the construction of "Tamper Resistant Barrier," "*Tamper/Tampering*" is defined as set forth in item #67, above.
72.	a first **secure** execution space, and	<u>secure</u>: see item #3 above	<u>secure</u>: see item #3 above

	'721 Claim 34	IT Construction	MS Construction
73.	at least one arrangement within the first **tamper resistant barrier** that prevents the first **secure** execution space from executing the same **executable** accessed by a second **secure** execution space having a second **tamper resistant barrier** with a second security level different from the first security level.	<u>tamper resistant barrier</u>: see item #71 above <u>secure</u>: see item #3 above <u>executable</u>: A computer program that can be run, directly or through interpretation.	<u>tamper resistant barrier</u>: see item #71 above <u>secure</u>: see item #3 above <u>executable</u>: A cohesive series of machine code instructions in a format that can be loaded into memory and run (executed) by a connected processor.

[illegible]. Patent No. 5,920,861, Asserted C[illegible]m 58

	'861 Claim 58	IT Construction	MS Construction
74.	58. A method of creating a first **secure container**, said method including the following steps;	The claim contains no requirement of a VDE. secure container: see item #57 above	Claim as a whole: The recited method is performed within a **VDE**. (See item #86 for Microsoft's construction of **VDE**.) secure container: see item #57 above
75.	accessing a descriptive data structure, said descriptive data structure including or addressing		
76.	organization information at least in part describing a required or desired organization of a content section of said first **secure container**, and	secure container: see item #57 above	secure container: see item #57 above
77.	metadata information at least in part specifying at least one step required or desired in creation of said first **secure container**;	secure container: see item #57 above	secure container: see item #57 above
78.	using said descriptive data structure to organize said first **secure container** contents;	secure container: see item #57 above	secure container: see item #57 above
79.	using said metadata information to at least in part determine specific information required to be included in said first **secure container** contents; and	secure container: see item #57 above	secure container: see item #57 above

	'861 Claim 58	IT Construction	MS Construction
80.	generating or identifying at least one rule designed to **control** at least one **aspect** of access to or **use** of at least a portion of said first **secure container** contents.	control (controlling): see item #7 above aspect: see item #60 above use: see item #42 above secure container: see item #57 above	control (controlling): see item #7 above aspect: see item #60 above use: see item #42 above secure container: see item #57 above

U.S. Patent No. 5,982,891, Asserted Claim: 1

	'891 Claim 1	IT Construction	MS Construction
81.	1. A method for using at least one resource processed in a **secure** operating environment at a first appliance, said method comprising:	The claim contains no requirement of a VDE. <u>secure</u>: see item #3 above	<u>Claim as a whole</u>: The recited method is performed within a **VDE**. (See item #86 for Microsoft's construction of **VDE**.) <u>secure</u>: see item #3 above
82.	**securely** receiving a first entity's **control** at said first appliance, said first entity being located remotely from said operating environment and said first appliance;	<u>securely (secure)</u>: see item #3 above <u>control</u>: see item #4 above	<u>securely (secure)</u>: see item #3 above <u>control</u>: see item #4 above
83.	**securely** receiving a second entity's **control** at said first appliance, said second entity being located remotely from said operating environment and said first appliance, said second entity being different from said first entity; and	<u>securely (secure)</u>: see item #3 above <u>control</u>: see item #4 above	<u>securely (secure)</u>: see item #3 above <u>control</u>: see item #4 above
84.	**securely** processing a data item at said first appliance, using at least one resource, including	<u>securely (secure)</u>: see item #3 above	<u>securely (secure)</u>: see item #3 above
85.	***securely** applying, at said first appliance through **use** of said at least one resource said first entity's **control** and said second entity's **control** to govern **use** of said data item.*	<u>securely (secure)</u>: see item #3 above <u>use</u>: see item #42 above <u>control</u>: see item #4 above <u>securely applying, at said first appliance through use of said at least one resource said first entity's control and said second entity's control to govern use of said data item</u>: Normal English, incorporating the separately defined terms: the first entity's Control	<u>securely (secure)</u>: see item #3 above <u>use</u>: see item #42 above <u>control</u>: see item #4 above <u>securely applying, at said first appliance through use of said at least one resource said first entity's control and said second entity's control to govern use of said data item</u>: (1) Processing the resource (component part of a first appliance's Secure

	'891 Claim 1	IT Construction	MS Construction
		and the second entity's Control are Securely applied to govern Use of the data item, the act of Securely applying involving use of the resource.	Operating Environment) within the Secure Operating Environment's special-purpose Secure Processing Unit (SPU) to execute the first **Control** and second **Control** in combination within the SPU. (2) This execution of these **Controls** governs (**Controls**) all **Use** of the data item by all users, processes, and devices. (3) The processing of the resource and execution of the **Controls** cannot be observed from outside the SPU and is performed only after the integrity of the resource and **Controls** is cryptographically verified. (4) A Secure Processing Unit is a special-purpose unit isolated from the rest of the world in which a hardware **Tamper Resistant Barrier** encapsulates a processor and internal **Secure** memory. (5) The processor cryptographically verifies the integrity of all code loaded from the **Secure** memory prior to execution, executes only the code that the processor has authenticated for its **Use**, and is otherwise **Secure**.

	'900 Claim 155	IT Construction	MS Construction
86.	155. A **virtual distribution environment** comprising	Virtual Distribution Evironment: This term is contained in the preamble of the claim and should not be defined, other than as requiring the individual claim elements. Without waiving its position that no separate definition is required, if required to propose such a definition, InterTrust proposes the following: secure, distributed electronic transaction management and rights protection system for controlling the distribution and/or other usage of electronically provided and/or stored information.	Claim as a Whole: The "virtual distribution environment" is **VDE**. Virtual Distribution Environment: (1) Data Security and Commerce World: InterTrust's February 13, 1995, patent application described as its "invention" a **Virtual Distribution Environment** ("VDE invention") for securing, administering, and auditing all security and commerce digital information within its multi-node world (community). **VDE** guarantees to all **VDE** "participants" identified in the patent application that it will limit all *Access* to and **Use** (i.e., interaction) of such information to authorized activities and amounts, will ensure any requested reporting of and payment for such **Use**, and will maintain the availability, secrecy, integrity, non-repudiation and authenticity of all such information present at any of its nodes (including protected content, information about content usage, and content **Controls**.). **VDE** is **Secure** against at least the threats identified in the Feburary 1995, patent application to this availability (no user may delete the information without authorization), secrecy (neither available nor disclosed to unauthorized persons or processes), integrity (neither intentional nor accidental alteration), non-repudiation (neither the receiver can disavow the receipt of a message nor can the sender disavow the origination of that message) and authenticity (asserted characteristics are genuine). **VDE** further provides and requires the components and capabilities described below. Anything less than or different than this is not **VDE** or the described "invention."

	'900 Claim 155	IT Construction	MS Construction
			(2) Secure Processing Environment: At each node where **VDE**-protected information is *Accessed*, **Used**, or assigned control information, **VDE** requires a *Secure Processing Environment* (as set forth in item #6). (3) VDE Controls: **VDE Allows** *Access* to or **Use** of protected information and processes only through execution of (and satisfaction of the requirements imposed by) **VDE Control(s)**. (4) VDE Secure Container: See construction of **Secure Container** (see item #57). (5) Non-Circumventable: **VDE** is non-circumventable (sequestered). It intercepts all attempts by any and all users, processes, and devices, to *Access* or **Use**, such as observing, interfering with, or removing) protected information, and prevents all such attempts other than as allowed by execution of (and satisfaction of all requirements imposed by) associated **VDE Controls** within *Secure Processing Environment(s)*. (6) Peer to Peer: **VDE** is peer-to-peer. Each **VDE** node has the innate ability to perform any role identified in the patent application (e.g., end user, content packager, distributor, **Clearinghouse**, etc.), and can protect information flowing in any direction between any nodes. **VDE** is not client-server. It does not pre-designate and restrict one or more nodes to act solely as a "server" (a provider of information (e.g., authored content, control information, etc.) to other nodes) or "client" (a requestor of such information). All types of protected-content transactions can proceed without requiring interaction with any server.

	'900 Claim 155	IT Construction	MS Construction
			(7) Comprehensive Range of Functions: **VDE** comprehensively governs (**Controls**) all security and commerce activities identified in the patent application, including (a) metering, budgeting, monitoring, reporting, and auditing information usage, (b) billing and paying for information usage, and (c) negotiating, signing and enforcing contracts that establish users' rights to *Access* or **Use** information. (8) User-Configurable: The specific protections governing (**Controlling)** specific **VDE**-protected information are specified, modified, and negotiated by **VDE**'s users. For example, **VDE** enables a consumer to place limits on the nature of content that may be *Accessed* at her node (e.g., no R-rated material) or the amount of money she can spend on viewing certain content, both subject only to other users' senior **Controls**. (9) General Purpose; Universal: **VDE** is universal as opposed to being limited to or requiring any particular type of appliance, information, or commerce model. It is a single, unified standard and environment within which an unlimited range of electronic rights protection, data security, electronic currency, and banking applications can run. (10) Flexible: **VDE** is more flexible than traditional information security and commerce systems. For example, **VDE** allows consumers to pay for only the user-defined portion of information that the user actually uses, and to pay only in proportion to any quantifiable **VDE** event (e.g., for only the number of paragraphs displayed from a book), and allows editing the content in **VDE** containers while maintaining its security.

	'900 Claim 155	IT Construction	MS Construction
			For the purposes of the construction of "VDE," "*Secure Processing Environment*" and "*Access*" are defined as set forth in item #4, above.
87.	a first **host processing environment** comprising	host processing environment: This term is explicitly defined in the claim and therefore needs no additional definition. It consists of those elements listed in the claim. Without waiving its position that no separate definition is required, if required to propose such a definition, InterTrust proposes the following: a Protected Processing Environment incorporating software-based security.	host processing environment: (1) A processing environment within a **VDE** node which is not a *Secure Processing Environment*. (2) A "host processing environment" may either be "secure" or "not secure." (3) A "secure host processing environment" is a self-contained **Protected Processing Environment**, formed by loaded, **Executable** programming executing on a general purpose CPU (not a Secure Processing Unit) running in protected (privileged) mode. (4) A "non-secure host processing environment" is formed by loaded, **Executable** programming executing on a general purpose CPU (not a Secure Processing Unit) running in user mode. For the purposes of the construction of "Host Processing Environment," a "*Secure Processing Environment*" is defined as set forth in item #4, above.
88.	a central processing unit;		
89.	main memory operatively connected to said central processing unit;		
90.	mass storage operatively connected to said central processing unit and said main memory;		

	'900 Claim 155	IT Construction	MS Construction
91.	said mass storage storing tamper resistant software designed to be loaded into said main memory and executed by said central processing unit, said tamper resistant software comprising:		
92.	machine check programming which ***derives information from one or more aspects of said host processing environment***,	derives: Normal English: obtains, receives or arrives at through a process of reasoning or deduction. In the context of computer operations, the "process of reasoning or deduction" constitutes operations carried out by the computer. aspect: see item #60 above host processing environment: see item #87 above derives information from one or more aspects of said host processing environment: Normal English, incorporating the separately defined terms: Derives (including creates) information based on at least one Aspect of the previously referred to Host Processing Environment.	derives: To retrieve from a specified source. aspect: see item #60 above host processing environment: see item #87 above derives information from one or more aspects of said host processing environment: (1) **Deriving** from the **Host Processing Environment** hardware one or more values that uniquely and persistently identify the **Host Processing Environment** and distinguish it from other **Host Processing Environments.** (2) The "one or more aspects of said host processing environment" are persistent elements or properties of the **Host Processing Environment** itself that are capable of being used to distinguish it from other environments, as opposed to, e.g., data or programs stored within the mass storage or main memory, or processes executing within the **Host Processing Environment.**
93.	one or more storage locations storing said information;		

	'900 Claim 155	IT Construction	MS Construction
94.	integrity programming which causes said machine check programming to **derive** said information, **compares** said information to information previously stored in said one or more storage locations, and	derive: see item #92 above compares: Normal English: examines for the purpose of noting similarities and differences. "Comparison" refers to the act of comparing.	derive: see item #92 above compares: A processor operation that evaluates two quantities and sets one of three flag conditions as a result of the comparison – greater than, less than, or equal to.
95.	generates an indication based on the result of said **comparison**; and	comparison (compares): see item #94 above	comparison (compares): see item #94 above
96.	programming which takes one or more actions based on the state of said indication;		
97.	said one or more actions including at least temporarily halting further processing.		

U.S. Patent No. 5,917,912, Asserted Claim: 8

	'912 Claim 8	IT Construction	MS Construction
98.	8. A process comprising the following steps:	The claim contains no requirement of a VDE.	Claim as a whole: The recited method is performed within a **VDE**. (See item #93 for Microsoft's construction of **VDE**.)
99.	accessing a first record **containing** information directly or indirectly identifying one or more elements of a first **component assembly**,	containing: see item #58 above component assembly: Components are code and/or data elements that are independently deliverable. A Component Assembly is two or more components associated together. Component Assemblies are utilized to perform operating system and/or applications tasks.	containing: see item #58 above component assembly: (1) A cohesive **Executable** component created by a channel which binds or links together two or more independently deliverable *Load Modules*, and associated data. (2) A **Component Assembly** is assembled, and executes, only within a **VDE** *Secure Processing Environment*. (3) A **Component Assembly** is assembled dynamically in response to, and to service, a particular content-related activity (e.g., a particular **Use** request). (4) Each **VDE Component Assembly** is assigned and dedicated to a particular activity, particular user(s), and particular protected information. (5) Each **Component Assembly** is independently assembled, loadable and deliverable vis-à-vis other **Component Assemblies**. (6) The dynamic assembly of a **Component Assembly** is directed by a "blueprint" *Record* **Containing** control information for this particular activity on this particular information by this particular user(s). (7) **Component Assemblies** are extensible and can be configured and reconfigured (modified) by all users, and combined by all users with other **Component Assemblies**, subject only to other users' "senior" **Controls**. For the purposes of the construction of "Component Assembly," "*Load Module*," "*Secure Processing Environment*" and "*Record*" are defined as set forth in item #4 above.
100.	at least one of said elements including at least some	executable programming (executable): see item #73 above	executable programming: A cohesive series of machine code instructions, comprising a computer program, in a

	'912 Claim 8	IT Construction	MS Construction
	executable programming,		format that can be loaded into memory and run (executed) by a connected processor. A "computer program" is a complete series of definitions and instructions that when executed on a computer will perform a required or requested task.
101.	at least one of said elements constituting a load module,		
102.	said load module including **executable programming** and a header;	executable programming (executable): see item #73 above	executable programming: see item #100 above
103.	said header including an execution space **identifier** *identifying at least one* ***aspect*** *of an execution space required for* ***use*** *and/or execution of the load module* associated with said header;	identifier: see item #28 aspect: see item #59 above use: see item #42 above identifying at least one aspect of an execution space required for use and/or execution of the load module: Normal English, incorporating the separately defined terms: identifying an Aspect (e.g. security level) of an execution space that is needed in order for the load module to execute or otherwise be used.	identifier: see item #28 aspect: see item #59 above use: see item #42 above identifying at least one aspect of an execution space required for use and/or execution of the load module: (1) Defining fully, without reference to any other information, at least one of the persistent elements or properties (**Aspects**) (that are capable of being used to distinguish it from other environments of an execution space) that are required for any **Use**, and/or for any execution, of the *Load Module*. (2) An execution space without all of those required aspects is incapable of making any such execution and/or other **Use** (e.g., **Copying**, displaying, printing) of the *Load Module*. For the purposes of the construction of this phrase, a "*Load Module*" is defined as set forth in item #4, above

	'912 Claim 8	IT Construction	MS Construction
104.	said execution space **identifier** provides the capability for distinguishing between execution spaces providing a higher level of security and execution spaces providing a lower level of security;	identifier: see item #28	identifier: see item #28
105.	using said information to identify and locate said one or more elements;		
106.	accessing said located one or more elements;		
107.	**securely** assembling said one or more elements to form at least a portion of said first **component assembly**;	securely: see item #3 above component assembly: see item #98 above	securely: see item #3 above component assembly: see item #98 above
108.	executing at least some of said **executable programming**; and	executable programming (executable): see item #73 above	executable programming: see item #100 above
109.	checking said record for validity prior to performing said executing step.		

U.S. Patent No. 5,917,912, Asserted Claim 35

	'912 Claim 35	IT Construction	MS Construction
110.	35. A process comprising the following steps:	The claim contains no requirement of a VDE.	Claim as a whole: The recited method is performed within a **VDE**. (See item #86 for Microsoft's construction of **VDE**.)
111.	at a first processing environment receiving a first record from a second processing environment remote from said first processing environment;		
112.	said first record being received in a **secure container**;	secure container: see item #57 above	secure container: see item #57 above
113.	said first record **containing** identification information directly or indirectly identifying one or more elements of a first **component assembly**;	containing: see item #57 above component assembly: see item #98 above	containing: see item #57 above component assembly: see item #98 above
114.	at least one of said elements including at least some **executable programming**;	executable programming (executable): see item #73 above	executable programming: see item #100 above
115.	said **component assembly** allowing access to or **use** of specified information;	component assembly: see item #98 above use: see item #42 above	component assembly: see item #98 above use: see item #42 above
116.	said **secure container** also including a first of said elements;	secure container: see item #57 above	secure container: see item #57 above
117.	accessing said first record;		
118.	using said identification information to identify and locate		

	'912 Claim 35	IT Construction	MS Construction
	said one or more elements;		
119.	said locating step including locating a second of said elements at a third processing environment located remotely from said first processing environment and said second processing environment;		
120.	accessing said located one or more elements;		
121.	said element accessing step including retrieving said second element from said third processing environment;		
122.	**securely** assembling said one or more elements to form at least a portion of said first **component assembly** specified by said first record; and	securely (secure): see item #3 above component assembly: see item #98 above	securely (secure): see item #3 above component assembly: see item #98 above
123.	executing at least some of said **executable programming,**	executable programming (executable): see item #73 above	executable programming: see item #100 above
124.	said executing step taking place at said first processing environment.		

EXHIBIT B

PLR 4-3(b) – The Parties' Construction of Disputed Terms & Phrases

	Claim Term/Phrase	InterTrust Construction	Microsoft Construction
1.	aspect 683.2 861.58 900.155 912.8	Feature, element, property or state.	An aspect of an environment is a persistent element or property of that environment that can be used to distinguish it from other environments.
2.	authentication 193.15	Identifying (e.g., a person, device, organization, document, file, etc.). Includes uniquely identifying or identifying as a member of a group.	To establish that the following asserted characteristics of something (e.g., a person, device, organization, document, file, etc.) are genuine: its identity, its data integrity, (i.e., it has not been altered) and its origin integrity (i.e., its source and time of origination).
3.	budget 193.1	Information specifying a limitation on usage.	(1) A unique type of "method" that specifies a decrementable numerical limitation on future Use (e.g., copying) of digital information and how such Use will be paid for, if at all. (2) A "method" is a collection of basic instructions, and information related to basic instructions, that provides context, data, requirements, and/or relationships for use in performing, and/or preparing to perform, basic instructions in relation to the operation of one or more electronic appliances.
4.	clearinghouse 193.19	A provider of financial and/or administrative services for a number of entities; or an entity responsible for the collection, maintenance, and/or distribution of materials, information, licenses, etc.	(1) A computer system that provides intermediate storing and forwarding services for both content and audit information, and which two or more parties trust to provide its services independently because it is operated under constraint of VDE security. (2) "Audit information" means all information created, stored, or reported in connection with an "auditing" process. "Auditing"

	Claim Term/Phrase	InterTrust Construction	Microsoft Construction
			means tracking, metering and reporting the usage of particular information or a particular appliance.
5.	compares 900.155	Normal English: examines for the purpose of noting similarities and differences.	A processor operation that evaluates two quantities and sets one of three flag conditions as a result of the comparison – greater than, less than, or equal to.
6.	component assembly 912.8, 912.35	Components are code and/or data elements that are independently deliverable. A Component Assembly is two or more components associated together. Component Assemblies are utilized to perform operating system and/or applications tasks.	(1) A cohesive **Executable** component created by a channel which binds or links together two or more independently deliverable *Load Modules* (see below), and associated data. (2) A **Component Assembly** is assembled, and executes, only within a **VDE** *Secure Processing Environment* (see below). (3) A **Component Assembly** is assembled dynamically in response to, and to service, a particular content-related activity (e.g., a particular **Use** request). (4) Each **VDE Component Assembly** is assigned and dedicated to a particular activity, particular user(s), and particular protected information. (5) Each **Component Assembly** is independently assembled, loadable and deliverable vis-à-vis other **Component Assemblies.** (6) The dynamic assembly of a **Component Assembly** is directed by a "blueprint" *Record* (see below) **Containing** control information for this particular activity on this particular information by this particular user(s). (7) **Component Assemblies** are extensible and can be configured and reconfigured (modified) by all users, and combined by all users with other **Component Assemblies,**

	Claim Term/Phrase	InterTrust Construction	Microsoft Construction
			subject only to other users' "senior" **Controls**. For the purposes of the construction of "Component Assembly," a "*Load Module*" is defined as follows: An **Executable**, modular unit of machine code (which may include data) suitable for loading into memory for execution by a processor. A load module is encrypted (when not within a secure processing unit) and has an **Identifier** that a calling process must provide to be able to use the load module. A load module is combinable with other load modules, and associated data, to form **Executable Component Assemblies**. A load module can execute only in a **VDE Protected Processing Environment**. Library routines are not load modules and dynamic link libraries are not load modules. For the purposes of the construction of "Component Assembly," a "*Secure Processing Environment*" is defined as follows: A Secure Processing Environment is uniquely identifiable, self-contained, non-circumventable, and trusted by all other **VDE** nodes to protect the availability, secrecy, integrity and authenticity of all information identified in the patent application as being protected, and to guarantee that such information will be accessed and **Used** only as expressly authorized by the associated **VDE Controls**, and to guarantee that all requested reporting of and payments for protected information use will be made. A Secure Processing

	Claim Term/Phrase	InterTrust Construction	Microsoft Construction
			Environment is formed by, and requires, a Secure Processing Unit having a hardware **Tamper Resistant Barrier** encapsulating a processor and internal **Secure** memory. The **Tamper Resistant Barrier** prevents all unauthorized interference, removal, observation, and other **Use** of the information and processes within it. For the purposes of the construction of "Component Assembly," a "*Record*" is defined as follows: A data structure that is a collection of fields (elements), each with its own name and type. Unlike an array, whose elements are accessed using an index, the elements of a record are accessed by name. A record can be accessed as a collective unit of elements, or the elements can be accessed individually.
7.	contain 683.2 912.8, 912.35	Normal English: to have within or to hold. In the context of an element contained within a data structure (e.g., a secure container), the contained element may be either directly within the container or the container may hold a reference indicating where the element may be found.	Physically (directly) storing within, as opposed to addressing (i.e., referring to something by the explicitly identified location where it is stored, without directly storing it).
8.	control (n.) 193.1, 193.11, 193.15, 193.19 683.2 891.1	Information and/or programming controlling operations on or use of resources (e.g., content) including (a) permitted, required or prevented operations, (b) the nature or extent of such operations or (c) the consequences of such operations.	(1) Independent, special-purpose, **Executable**, which can execute only within a *Secure Processing Environment.* (2) Each **VDE Control** is a **Component Assembly** dedicated to a particular activity (e.g., editing, modifying another **Control**, a user-defined action, etc.), particular user(s), and particular protected information, and whose satisfactory execution is necessary to *Allowing* (see below) that activity.

	Claim Term/Phrase	InterTrust Construction	Microsoft Construction
			(3) Each separate information *Access* (see below) or **Use** is independently **Controlled** by independent **VDE Control(s)**. (4) Each **VDE Control** is assembled within a *Secure Processing Environment* from independently deliverable modular components (e.g., *Load Modules* or other **Controls**), dynamically in response to an information *Access* or **Use** Request. (5) The dynamic assembly of a **Control** is directed by a "blueprint" *Record* (put in place by one or more **VDE** users) **Containing** control information identifying the exact modular code components to be assembled and executed to govern (i.e., **Control**) this particular activity on this particular information by this particular user(s). (6) Each **Control** is independently assembled, loaded and delivered vis-à-vis other **Controls**. (7) Control information and **Controls** are extensible and can be configured and modified by all users, and combined by all users with any other **VDE** control information or **Controls** (including that provided by other users), subject only to "senior" user **Controls**. (8) Users can assign control information (including alternative control information) and **Controls** to an arbitrarily fine, user-defined portion of the protected information, such as a single paragraph of a document, as opposed to being limited to file-based controls. (9) **VDE Controls** reliably limit Use of the protected information to only authorized activities and amounts.

	Claim Term/Phrase	InterTrust Construction	Microsoft Construction
			For the purposes of the construction of "Control," a "*Secure Processing Environment*" is defined as set forth in item #6, above. For the purposes of the construction of "Control," "*Allowing*" is defined as follows: Actively permitting an action that otherwise cannot be taken (i.e., is prohibited) by any user, process, or device. In **VDE**, an action is allowed only through execution (within a *Secure Processing Environment*) of the **VDE Control(s)** assigned to the particular action request, and satisfaction of all requirements imposed by such execution. For the purposes of the construction of "Control," "*Access*" is defined as follows: To satisfactorily perform the steps necessary to obtain something so that it can be **Used** in some manner (e.g., for information: copied, printed, decrypted, encrypted, saved, modified, observed, or moved, etc.). In **VDE**, access to protected information is achieved only through execution (within a *Secure Processing Environment*) of the **VDE Control(s)** assigned to the particular "access" request, satisfaction of all requirements imposed by such execution, and the **Controlled** opening of the **Secure Container Containing** the information. For the purposes of the construction of "Control," "*Load Module*" and "*Record*" are defined as set forth in item #6, above.
9.	controlling, control (v.)	Normal English: to exercise authoritative or dominating influence over; direct.	(1) Reliably defining and enforcing the conditions and requirements under which an action that otherwise

	Claim Term/Phrase	InterTrust Construction	Microsoft Construction
	193.1 861.58		cannot be taken, will be *Allowed*, and the manner in which it may occur. Absent verified satisfaction of those conditions and requirements, the action cannot be taken by any user, process or device. (2) In **VDE**, an action is **Controlled** through execution of the applicable **VDE Control(s)** within a **VDE** *Secure Processing Environment*. (3) More specifically, in **VDE**, **Controlling** is effected by use of **VDE Controls**, **VDE Secure Containers**, and **VDE** foundation (including **VDE** *Secure Processing Environment*, "object registration," and other mechanisms for allegedly individually ensuring that specific **Controls** are enforced vis-à-vis specific objects (and their content at an arbitrary granular level) and specific "users"). For the purposes of the construction of "Control (v.)" et al, "*Allowed*" is defined as set forth in item #8, above, and "*Secure Processing Environment*" is defined as set forth in item #6, above.
10.	copy, copied, copying 193.1, 193.11, 193.15, 193.19	Reproduce, reproduced, reproducing. The reproduction must be usable, may incorporate all of the original item or only some of it, and may involve some changes to the item as long as the essential nature of the content remains unchanged.	(1) To reproduce all of a *Digital File* or other complete physical block of data from one location on a storage medium to another location on the same or different storage medium, leaving the original block of data unchanged, such that two distinct and independent objects exist. (2) Although the layout of the data values in physical storage may differ from the original, the resulting "copy" is logically indistinguishable from the original. (3) The resulting "copy" may or may not be encrypted, ephemeral, usable, or accessible.

	Claim Term/Phrase	InterTrust Construction	Microsoft Construction
			For the purposes of the construction of "Copy," et al, a "*Digital File*" is defined as: A named, static unit of storage allocated by a "file system" and **Containing** digital information. A digital file enables any application using the "file system" to randomly access its contents and to distinguish it by name from every other such unit. A copy of a digital file is a separate digital file. A "file system" is the portion of the operating system that translates requests made by application programs for operations on "files" into low-level tasks that can control storage devices such as disk drives.
11.	derive 900.155	Normal English: obtain, receive or arrive at through a process of reasoning or deduction. In the context of computer operations, the "process of reasoning or deduction" constitutes operations carried out by the computer.	To retrieve from a specified source.
12.	designating 721.1	Normal English: indicating, specifying, pointing out or characterizing.	Designating something for a particular **Use** means specifying it for and restricting it to that **Use**.
13.	device class 721.1	A group of devices which share at least one attribute.	The generic name for a group of device types. For example, all display stations belong to the same device class. A device class is different from a device type. A device type is composed of all devices that share a common model number or family (e.g. IBM 4331 printers).
14.	digital signature, digitally signing 721.1	digital signature: A digital value, verifiable with a key, that can be used to determine the source and/or integrity of a signed item (e.g., a file, program, etc.). Digitally signing is the process of creating a digital signature.	<u>digital signature</u>: A computationally unforgeable string of characters (e.g., bits) generated by a cryptographic operation on a block of data using some secret. The string can be generated only by an entity that knows the secret, and hence provides evidence that the

	Claim Term/Phrase	InterTrust Construction	Microsoft Construction
			entity must have generated it. digitally signing: (1) Creating a **Digital Signature** using a secret *Key* (see below). (2) In symmetric key cryptography, a "secret key" is a *Key* that is known only to the sender and recipient. In asymmetric key cryptography, a "secret key" is the private *Key* of a public/private key pair, in which the two keys are related uniquely by a predetermined mathematical relationship such that it is computationally infeasible to determine one from the other. For the purposes of the construction of "Digital Signature" and "Digital Signing," a "*Key*" is defined as: A bit sequence used and needed by a cryptographic algorithm to encrypt a block of plain text or to decrypt a block of cipher text. A key is different from a key seed or other information from which the actual encryption and/or decryption key is constructed, **Derived**, or otherwise identified. In symmetric key cryptography, the same key is used for both encryption and decryption. In asymmetric or "public key" cryptography, two related keys are used; a block of text encrypted by one of the two keys (e.g., the "public key") can be decrypted only by the corresponding key (e.g., the "private key").
15.	executable programming, executable 721.34 912.8, 912.35	A computer program that can be run, directly or through interpretation.	executable: A cohesive series of machine code instructions in a format that can be loaded into memory and run (executed) by a connected processor.

	Claim Term/Phrase	InterTrust Construction	Microsoft Construction
			<u>executable programming</u>: A cohesive series of machine code instructions, comprising a computer program, in a format that can be loaded into memory and run (executed) by a connected processor. A "computer program" is a complete series of definitions and instructions that when executed on a computer will perform a required or requested task.
16.	host processing environment 900.155	This term is explicitly defined in the claim and therefore needs no additional definition. It consists of those elements listed in the claim. Without waiving its position that no separate definition is required, if required to propose such a definition, InterTrust proposes the following: a Protected Processing Environment incorporating software-based security.	(1) A processing environment within a **VDE** node which is not a *Secure Processing Environment*. (2) A "host processing environment" may either be "secure" or "not secure." (3) A "secure host processing environment" is a self-contained **Protected Processing Environment**, formed by loaded, **Executable** programming executing on a general purpose CPU (not a Secure Processing Unit) running in protected (privileged) mode. (4) A "non-secure host processing environment" is formed by loaded, **Executable** programming executing on a general purpose CPU (not a Secure Processing Unit) running in user mode. For the purposes of the construction of "host processing environment," a "*Secure Processing Environment*" is defined as set forth in item #6, above.
17.	identifier 193.15 912.8	Information used to identify something or someone (e.g., a password). In this definition, "identify" means to establish the identity of or to ascertain the origin, nature, or	Any text string used as a label naming an individual instance of what it *Identifies*. For the purpose of the construction of "Identifier," "Identify" is defined as: To establish as being a particular

	Claim Term/Phrase	InterTrust Construction	Microsoft Construction
		definitive characteristics of; includes identifying as an individual or as a member of a group.	instance of a person or thing.
18.	protected processing environment 683.2 721.34	An environment in which processing and/or data is at least in part protected from tampering. The level of protection can vary, depending on the threat. In this definition, "environment" means capabilities available to a program running on a computer or other device or to the user of a computer or other device. Depending on the context, the environment may be in a single device (e.g., a personal computer) or may be spread among multiple devices (e.g., a network).	(1) A uniquely identifiable, self-contained computing base trusted by all **VDE** nodes to protect the availability, secrecy, integrity and authenticity of all information identified in the February, 1995, patent application as being protected, and to guarantee that such information will be *Accessed* and **Used** only as expressly authorized by **VDE Controls**. (2) At most **VDE** nodes, the **Protected Processing Environment** is a *Secure Processing Environment* which is formed by, and requires, a hardware **Tamper Resistant Barrier** encapsulating a special-purpose Secure Processing Unit having a processor and internal secure memory. "Encapsulated" means hidden within an object so that it is not directly accessible but rather is accessible only through the object's restrictive interface. (3) The **Tamper Resistant Barrier** prevents all unauthorized (intentional or accidental) interference, removal, observation, and use of the information and processes within it, by all parties (including all users of the device in which the **Protected Processing Environment** resides), except as expressly authorized by **VDE Controls**. (4) A **Protected Processing Environment** is under **Control** of **Controls** and control information provided by one or more parties, rather than being under **Control** of the appliance's users or programs. (5) Where a **VDE** node is an

	Claim Term/Phrase	InterTrust Construction	Microsoft Construction
			established financial **Clearinghouse**, or other such facility employing physical facility and user-identity **Authentication** security procedures trusted by all **VDE** nodes, and the **VDE** node does not *Access* or Use **VDE**-protected information, or assign **VDE** control information, then the **Protected Processing Environment** at that **VDE** node may instead be formed by a general-purpose CPU that executes all **VDE** "security" processes in protected (privileged) mode. (6) A **Protected Processing Environment** requires more than just verifying the integrity of **Digitally Signed Executable** programming prior to execution of the programming; or concealment of the program, associated data, and execution of the program code; or use of a password as its protection mechanism. For the purposes of the construction of "Protected Processing Environment," a "*Secure Processing Environment*" is defined as set forth in item #6, above, and "*Access*" is defined as set forth in item #8, above.

	Claim Term/Phrase	InterTrust Construction	Microsoft Construction
19.	secure, securely 193.1, 193.11, 193.15 683.2 721.34 861.58 891.1 912.8, 912.35	One or more mechanisms are employed to prevent, detect or discourage misuse of or interference with information or processes. Such mechanisms may include concealment, Tamper Resistance, Authentication and access control. Concealment means that it is difficult to read information (for example, programs may be encrypted). Tamper Resistance and Authentication are separately defined. Access control means that access to information or processes is limited on the basis of authorization. Security is not absolute, but is designed to be sufficient for a particular purpose.	(1) A state in which all users of a system are guaranteed that all information, processes, and devices within the system, shall have their availability, secrecy, integrity, authenticity and nonrepudiation maintained against all of the identified threats thereto. (2) "Availability" means the property that information is accessible and usable upon demand by authorized persons, at least to the extent that no user may delete the information without authorization. (3) "Secrecy," also referred to as confidentiality, means the property that information (including computer processes) is not made available or disclosed to unauthorized persons or processes. (4) "Integrity" means the property that information has not been altered either intentionally or accidentally. (5) "Authenticity" means the property that the characteristics asserted about a person, device, program, information, or process are genuine and timely, particularly as to identity, data integrity, and origin integrity. (6) "Nonrepudiation" means the property that a sender of information cannot deny its origination and that a recipient of information cannot deny its receipt.
20.	secure container 683.2 861.58 912.35	A container that is Secure. In this definition, "container" means a digital file containing linked and/or embedded items.	(1) A **VDE Secure Container** is a self-contained, self-protecting data structure which (a) encapsulates information of arbitrary size, type, format, and organization, including other, nested, containers, (b) cryptographically protects that information from all unauthorized *Access* and Use, (c) provides encrypted storage management

	Claim Term/Phrase	InterTrust Construction	Microsoft Construction
			functions for that information, such as hiding the physical storage location(s) of its protected contents, (d) permits the association of itself or its contents with **Controls** and control information governing (**Controlling**) *Access* to and **Use** thereof, and (e) prevents such **Use** or *Access* (as opposed to merely preventing decryption) until it is "opened." (2) A **Secure Container** can be opened only as expressly *Allowed* by the associated **VDE Control(s)**, only within a *Secure Processing Environment*, and only through decryption of its encrypted header. (3) A **Secure Container** is not directly accessible to any non-**VDE** or user calling process. All such calls are intercepted by **VDE**. (4) The creator of a **Secure Container** can assign (or allow others to assign) control information to any arbitrary portion of a **Secure Container**'s contents, or to an empty **Secure Container** (to govern (**Control**) the later addition of contents to the container, and *Access* to or **Use** of those contents). (5) A container is not a **Secure Container** merely because its contents are encrypted and signed. A **Secure Container** is itself **Secure**. (6) All **VDE**-protected information (including protected content, information about content usage, content-control information, **Controls**, and *Load Modules*) is encapsulated within a **Secure Container** whenever stored outside a *Secure Processing Environment* or secure database.

	Claim Term/Phrase	InterTrust Construction	Microsoft Construction
			For the purposes of the construction of "Secure Container," "*Secure Processing Environment*" and "*Load Module*" are defined as set forth in item #6, above, and "*Access*" and "*Allow*" are defined as set forth in item #8, above.
21.	tamper resistance 721.1	Making tampering more difficult and/or allowing detection of tampering. In this definition, "tampering" means using (e.g., observing or altering) in any unauthorized manner, or interfering with authorized use.	tamper resistance: The ability of a **Tamper Resistant Barrier** to prevent *Access*, observation, and interference with information or processing encapsulated by the barrier. For the purposes of the construction of "Tamper Resistance," "*Tamper/Tampering*" is defined as: Using (e.g., observing or altering) in any unauthorized manner, or interfering with authorized use. For the purposes of the construction of "Tamper Resistance," "*Access*" is defined as set forth in item # 6, above.
22.	tamper resistant barrier 721.34	Hardware and/or software that provides Tamper Resistance.	(1) An active device that encapsulates and separates a **Protected Processing Environment** from the rest of the world. (2) It prevents information and processes within the **Protected Processing Environment** from being observed, interfered with, and leaving except under appropriate conditions ensuring security. (3) It also **Controls** external access to the encapsulated **Secure** resources, processes and information. (4) A **Tamper Resistant Barrier** is capable of destroying protected information in response to *Tampering* attempts. For the purposes of the construction

	Claim Term/Phrase	InterTrust Construction	Microsoft Construction
			of "Tamper Resistant Barrier," "*Tamper/Tampering*" is defined as set forth in item #21, above.
23.	use 193.19 683.2 721.1 861.58 891.1 912.8, 912.35	Normal English: to put into service or apply for a purpose, to employ.	(1) To use information is to perform some action on it or with it (e.g., copying, printing, decrypting, encrypting, saving, modifying, observing, or moving, etc.). (2) In **VDE**, information **Use** is *Allowed* only through execution of the applicable **VDE Control(s)** and satisfaction of all requirements imposed by such execution. For the purposes of the construction of "Use," "*Allowed*" is defined as set forth in item #8 above.
24.	virtual distribution environment 900.155 Also as set forth in each "claim as a whole" by Microsoft.	This term is contained in the preamble of the claim and should not be defined, other than as requiring the individual claim elements. The term "virtual distribution environment" should not be read into claims that do not actually recite it. Without waiving its position that no separate definition is required, if required to propose such a definition, InterTrust proposes the following: secure, distributed electronic transaction management and rights protection system for controlling the distribution and/or other usage of electronically provided and/or stored information.	<u>VDE/Virtual Distribution Environment</u>: (1) <u>Data Security and Commerce World</u>: InterTrust's February 13, 1995, patent application described as its "invention" a **Virtual Distribution Environment** ("VDE invention") for securing, administering, and auditing all security and commerce digital information within its multi-node world (community). **VDE** guarantees to all **VDE** "participants" identified in the patent application that it will limit all *Access* to and **Use** (i.e., interaction) of such information to authorized activities and amounts, will ensure any requested reporting of and payment for such **Use**, and will maintain the availability, secrecy, integrity, non-repudiation and authenticity of all such information present at any of its nodes (including protected content, information about content usage, and content **Controls**.).

	Claim Term/Phrase	InterTrust Construction	Microsoft Construction
			VDE is **Secure** against at least the threats identified in the Feburary 1995, patent application to this availability (no user may delete the information without authorization), secrecy (neither available nor disclosed to unauthorized persons or processes), integrity (neither intentional nor accidental alteration), non-repudiation (neither the receiver can disavow the receipt of a message nor can the sender disavow the origination of that message) and authenticity (asserted characteristics are genuine). **VDE** further provides and requires the components and capabilities described below. Anything less than or different than this is not **VDE** or the described "invention." (2) <u>Secure Processing Environment</u>: At each node where **VDE**-protected information is *Accessed*, **Used**, or assigned control information, **VDE** requires a *Secure Processing Environment* (as set forth in item #6). (3) <u>VDE Controls</u>: **VDE Allows** *Access* to or **Use** of protected information and processes only through execution of (and satisfaction of the requirements imposed by) **VDE Control(s)**. (4) <u>VDE Secure Container</u>: See construction of **Secure Container**. (5) <u>Non-Circumventable</u>: **VDE** is non-circumventable (sequestered). It intercepts all attempts by any and all users, processes, and devices, to *Access* or **Use**, such as observing, interfering with, or removing) protected information, and prevents all such attempts other than as

	Claim Term/Phrase	InterTrust Construction	Microsoft Construction
			allowed by execution of (and satisfaction of all requirements imposed by) associated **VDE Controls** within *Secure Processing Environment(s)*. (6) Peer to Peer: **VDE** is peer-to-peer. Each **VDE** node has the innate ability to perform any role identified in the patent application (e.g., end user, content packager, distributor, **Clearinghouse**, etc.), and can protect information flowing in any direction between any nodes. **VDE** is not client-server. It does not pre-designate and restrict one or more nodes to act solely as a "server" (a provider of information (e.g., authored content, control information, etc.) to other nodes) or "client" (a requestor of such information). All types of protected-content transactions can proceed without requiring interaction with any server. (7) Comprehensive Range of Functions: **VDE** comprehensively governs (**Controls**) all security and commerce activities identified in the patent application, including (a) metering, budgeting, monitoring, reporting, and auditing information usage, (b) billing and paying for information usage, and (c) negotiating, signing and enforcing contracts that establish users' rights to *Access* or **Use** information. (8) User-Configurable: The specific protections governing (**Controlling**) specific **VDE**-protected information are specified, modified, and negotiated by **VDE**'s users. For example, **VDE** enables a consumer to place limits on the nature of content that may be *Accessed* at her

	Claim Term/Phrase	InterTrust Construction	Microsoft Construction
			node (e.g., no R-rated material) or the amount of money she can spend on viewing certain content, both subject only to other users' senior **Controls**. (9) General Purpose; Universal: **VDE** is universal as opposed to being limited to or requiring any particular type of appliance, information, or commerce model. It is a single, unified standard and environment within which an unlimited range of electronic rights protection, data security, electronic currency, and banking applications can run. (10) Flexible: **VDE** is more flexible than traditional information security and commerce systems. For example, **VDE** allows consumers to pay for only the user-defined portion of information that the user actually uses, and to pay only in proportion to any quantifiable **VDE** event (e.g., for only the number of paragraphs displayed from a book), and allows editing the content in **VDE** containers while maintaining its security. For the purposes of the construction of "VDE," a "*Secure Processing Environment*" is defined as set forth in item #6, above. For the purposes of the construction of "VDE," "*Access*" is defined as set forth in item #8, above.
25.	193.1: "a budget specifying the number of copies which can be made of said digital file"	Normal English, incorporating the separately defined terms: a Budget stating the number of copies that can be made of the digital file referred to earlier in the claim.	A **Budget** explicitly stating the total number of copies (whether or not decrypted, long-lived, or accessible) that (since creation of the **Budget**) are authorized to be made of the *Digital File* by any and all users, devices, and processes. No process,

	Claim Term/Phrase	InterTrust Construction	Microsoft Construction
			user, or device is able to make another copy of the *Digital File* once this number of copies has been made. For the purposes of the construction of this phrase, "*Digital File*" is defined as set forth in item #6, above.
26.	193.1: "controlling the copies made of said digital file"	The nature of this operation is further defined in later claim elements. In context, the copy control determines the conditions under which a digital file may be Copied and the copied file stored on a second device.	**Controlling Uses** of and *Accesses* to all copies of the *Digital File*, by all users, processes, and devices, by executing each of the recited "at least one" **Copy Control(s)** within **VDE** *Secure Processing Environment(s)*. Each **Control** governs **(Controls)** only one action, which action may or may not differ among the different "at least one" **Controls**. All **Uses** and *Accesses* are prohibited and incapable of occurring except to the extent *Allowed* by the "at least one" **Copy Control(s)**. For the purposes of the construction of this phrase, a "*Secure Processing Environment*" is defined as set forth in item #6, above, and "*Access*" and "*Allowed*" are defined as set forth in item #8, above.
27.	721.1: "digitally signing a second load module with a second digital signature different from the first digital signature, the second digital signature designating the second load module for use by a second device class having at least one of tamper resistance	Normal English, incorporating the separately defined terms: generating a Digital Signature for the second load module, the Digital Signature Designating that the second load module is for use by a second Device Class. This element further requires that the second Device Class have a different Tamper Resistance or security level than the first Device Class.	(1) **Digitally Signing** a different ("second") *Load Module* by using a different ("second") **Digital Signature** as the signature *Key*, which signing indicates to any and all devices in the second **Device Class** that the signor authorized and restricted this *Load Module* for **Use** by that device. (2) No **VDE** device can perform any execution of any *Load Module* without such authorization. The method ensures that the *Load Module* cannot execute in a particular **Device Class** and ensures

	Claim Term/Phrase	InterTrust Construction	Microsoft Construction
	and security level different from the at least one of tamper resistance and security level of the first device class"		that no device in that **Device Class** has the *Key(s)* necessary to verify the **Digital Signature**. (3) All devices in the first **Device Class** have the same persistent (not just occasional) and identified level of **Tamper Resistance** and the same persistent and identified level of security. All devices in the second **Device Class** have the same persistent and identified level of **Tamper Resistance** and same persistent and identified level of security. (4) The identified level of **Tamper Resistance** or identified level of security (or both) for the first **Device Class**, is greater than or less than the identified level of **Tamper Resistance** or identified level of security for the second **Device Class**. For the purposes of the construction of this phrase, a "*Load Module*" is defined as set forth in item #6, above, and "*Key*" is defined as set forth in item #14, above.
28.	891.1: "securely applying, at said first appliance through use of said at least one resource said first entity's control and said second entity's control to govern use of said data item"	Normal English, incorporating the separately defined terms: the first entity's Control and the second entity's Control are Securely applied to govern Use of the data item, the act of Securely applying involving use of the resource.	(1) Processing the resource (component part of a first appliance's **Secure** Operating Environment) within the **Secure** Operating Environment's special-purpose Secure Processing Unit (SPU) to execute the first **Control** and second **Control** in combination within the SPU. (2) This execution of these **Controls** governs (**Controls**) all **Use** of the data item by all users, processes, and devices. (3) The processing of the resource and execution of the **Controls** cannot be observed from outside the SPU and is performed only after the

	Claim Term/Phrase	InterTrust Construction	Microsoft Construction
			integrity of the resource and **Controls** is cryptographically verified. (4) A Secure Processing Unit is a special-purpose unit isolated from the rest of the world in which a hardware **Tamper Resistant Barrier** encapsulates a processor and internal **Secure** memory. (5) The processor cryptographically verifies the integrity of all code loaded from the **Secure** memory prior to execution, executes only the code that the processor has authenticated for its **Use**, and is otherwise **Secure**.
29.	900.155: "derives information from one or more aspects of said host processing environment"	Normal English, incorporating the separately defined terms: Derives (including creates) information based on at least one Aspect of the previously referred to Host Processing Environment	(1) **Deriving** from the **Host Processing Environment** hardware one or more values that uniquely and persistently identify the **Host Processing Environment** and distinguish it from other **Host Processing Environments.** (2) The "one or more aspects of said host processing environment" are persistent elements or properties of the **Host Processing Environment** itself that are capable of being used to distinguish it from other environments, as opposed to, e.g., data or programs stored within the mass storage or main memory, or processes executing within the **Host Processing Environment.**
30.	912.8: "identifying at least one aspect of an execution space required for use and/or execution of the load module"	Normal English, incorporating the separately defined terms: identifying an Aspect (e.g. security level) of an execution space that is needed in order for the load module to execute or otherwise be used.	(1) Defining fully, without reference to any other information, at least one of the persistent elements or properties (**Aspects**) (that are capable of being used to distinguish it from other environments of an execution space) that are required for any **Use**, and/or for any execution, of the *Load Module*. (2) An execution space without all of those required aspects is

	Claim Term/Phrase	InterTrust Construction	Microsoft Construction
			incapable of making any such execution and/or other **Use** (e.g., **Copying**, displaying, printing) of the *Load Module*. For the purposes of the construction of this phrase, a "*Load Module*" is defined as set forth in item #6, above.

EXHIBIT C

PLR 4-3(b) – Identification of Supporting Evidence

The following represents InterTrust's list of evidence relevant to construction of the disputed terms and phrases.

Notes:

1. InterTrust reserves the right to supplement this list as needed to respond to changed constructions proffered by Microsoft. InterTrust also reserves the right to rely on evidence cited in the original version of this Exhibit, filed February 3, 2003.

2. In the following list, certain terms and phrases include other, separately defined terms. In such cases, the evidence supporting the separately defined term is also relevant to construction of the larger term.

3. The InterTrust patents include overlapping specifications, in which the same text may be found in two or more specifications. Where only one of the specifications is cited, InterTrust reserves the right to substitute citations for the same text in the other specifications.

4. Highlighting has been used to indicate added emphasis.

5. Each claim term is followed by a list of all patent claims in which the term appears (e.g., "193.15" means claim 15 from the '193 patent).

Key to abbreviations:
- USP = United States Patent
- '193 patent = USP 6,253,193
- '683 patent = USP 6,185,683
- '721 patent = USP 6,157,721
- '891 patent = USP 5,982,891
- '861 patent = USP 5,920,861
- '912 patent = USP 5,917,912
- '900 patent = USP 5,892,900

	Claim Term / Phrase	InterTrust Evidence
1.	aspect 683.2, 861.58, 900.155, 912.8	**Patent Specifications** **1(A)** This reinitialization mechanism would permit CPU/SPU 2650 to be initialized several times, facilitating testing and/or re-use for different applications, while protecting all security-relevant aspects of its operation. '900 patent at 77:15-19. **1(B)** In addition, the overall software-based tamper resistant barrier 674 and associated PPE system is sufficiently complex so that it is difficult to tamper with a part of it without destroying other aspects of its functionality (i.e., a "defense in depth"). '900 patent at 236:3-7. **1(C)** As with any system incorporating "applications" and "operating systems," the boundary between these aspects of an overall system can be ambiguous. '193 patent at 83:30-32. **1(D)** Since SPE 503 in the preferred embodiment runs within the confines of an SPU 500, one aspect of this device driver 736 is to provide low level communications services with the SPU 500 hardware. '193 patent at 95:27-30. **1(E)** Templates may present one or more models that describe various

	Claim Term / Phrase	InterTrust Evidence
		aspects of a content object and how the object should be created including employing secure atomic methods that are used to create, alter, and/or destroy permissions records 808 and/or associated budgets, etc. '193 patent at 260:42-47. **1(F)** In accordance with one aspect of how to advantageously use descriptive data structures in accordance with a preferred embodiment of this invention, a machine readable descriptive data structure may be created by a provider to describe the layout of the provider's particular rights management data structure(s) such as secure containers. '861 patent at 6:24-29. **1(G)** Controls 316 may provide rules and associated consequences for controlling or otherwise affecting the use or other aspects of what value chain participant 602 can do with DDS 200. '861 patent at 17:3-6.

	Claim Term / Phrase	InterTrust Evidence
2.	**authentication** 193.15	**<u>Patent Specifications</u>** **2(A)** To increase the security of security barrier 502 even further, it is possible to encase or include SPU 500 in one or more further physical enclosures such as, for example: epoxy or other "potting compound"; further module enclosures including additional self-destruct, self-disabling or other features activated when tampering is detected; further modules providing additional security protections such as requiring password or other authentication to operate; and the like. '193 patent at 64:29-37. **2(B)** It may also or alternatively provide or include one or more passwords or other information used to identify or otherwise verify/authenticate an individual's identity, such as voice print and retinal scan information. '193 patent at 236:21-25. **2(C)** This certification process in the preferred embodiment may be used to permit a VDE electronic appliance to present one or more "certificates" authenticating that it (or its key) can be trusted. As described above, this "certification" process may be used by one PPE 650 to "certify" that it is an authentic VDE PPE, it has a certain level of security and capability set (e.g., it is hardware based rather than merely software based), etc. Briefly, the "certification" process may involve using a certificate private key of a certification key pair to encrypt a message including another VDE node's public-key. The private key of a certification key pair is preferably used to generate a PPE certificate. It is used to encrypt a public-key of the PPE. A PPE certificate can either be stored in the PPE, or it may be stored in a certification repository. '193 patent at 213:1-15.

	Claim Term / Phrase	InterTrust Evidence
		2(D) SPE Authentication Manager/Service Communications Manager 564 The Authentication Manager/Service Communications Manager 564 supports calls for user password validation and "ticket" generation and validation. It may also support secure communications between SPE 503 and an external node or device (e.g., a VDE administrator or distributor). It may support the following examples of authentication-related service requests in the preferred embodiment: **Call Name** — **Description** <u>User Services</u> Create User — Creates a new user and stores Name Services Records (NSRs) for use by the Name Services Manager 752. Authenticate User — Authenticates a user for use of the system. This request lets the caller authenticate as a specific user ID. Group membership is also authenticated by this request. The authentication returns a "ticket" for the user. '193 patent at 123:21-42.

	Claim Term / Phrase	InterTrust Evidence
3.	**budget** 193.1	**<u>Patent Specifications</u>** **3(A)** PERC 808 may also contain or refer to budgets containing potentially valuable quantities/values. Such budgets may be stored within a traveling object itself, or they may be delivered separately and protected by highly secure communications keys and administrative object keys and management database techniques. '193 patent at 132:60-65. **3(B)** User Data Elements (UDEs) 1200 and Method Data Elements (MDEs) 1202 in the preferred embodiment store data. There are many types of UDEs 1200 and MDEs 1202 provided by the preferred embodiment. In the preferred embodiment, each of these different types of data structures shares a common overall format including a common header definition and naming scheme. Other UDEs 1200 that share this common structure include "local name services records" (to be explained shortly) and account information for connecting to other VDE participants. These elements are not necessarily associated with an individual user, and may therefore be considered MDEs 1202. All UDEs 1200 and all MDEs 1202 provided by the preferred embodiment may, if desired, (as shown in Figure 16) be stored in a common physical table within secure database 610, and database access processes may commonly be used to access all of these different types of data structures. In the preferred embodiment, PERCs 808 and user rights table records are types of UDE 1200. There are many other types of UDEs 1200/MDEs 1202, including for example, meters, meter trails, budgets, budget trails, and audit trails. '193 patent at 142:41-61. **3(C)** In the example shown in Figure 41d, a distributor at a VDE distributor node (106) might request budget from a content creator at another node (102). This request may be made in the context of a secure VDE communication or it may be passed in an "out-of-

	Claim Term / Phrase	InterTrust Evidence
		channel" communication (e.g. a telephone call or letter). The creator 102 may decide to grant budget to the distributor 106 and processes a distribute event (1452 in BUDGET method 1510 at VDE node 102). A result of processing the distribute event within the BUDGET method might be a secure communication (1454) between VDE nodes 102 and 106 by which a budget granting use and redistribute rights to the distributor 106 may be transferred from the creator 102 to the distributor. The distributor's VDE node 106 may respond to the receipt of the budget information by processing the communication using the reply process 1475B of the BUDGET method 1510. The reply event processing 1475B might, for example, install a budget and PERC 808 within the distributor's VDE 106 node to permit the distributor to access content or processes for which access is control at least in part by the budget and/or PERC. At some point, the distributor 106 may also desire to use the content to which she has been granted rights to access. After registering to use the content object, the user 112 would be required to utilize an array of "use" processes 1476C to, for example, open, read, write, and/or close the content object as part of the use process. Once the distributor 106 has used some or all of her budget, she may desire to obtain additional budget. The distributor 106 might then initiate a process using the BUDGET method request process (1480B). Request process 1480B might initiate a communication (1482AB) with the content creator VDE node 102 requesting more budget and perhaps providing details of the use activity to date (e.g., audit trails). The content creator 102 processes the 'get more budget' request event 1482AB using the response process (1484A) within the creator's BUDGET method 1510A. Response process 1484A might, for example, make a determination if the use information indicates proper use of the content, and/or if the distributor is credit worthy for more budget. The BUDGET method response process 1484A might also initiate a financial transaction to transfer funds from the distributor to pay for said use, or use the distribute process 1472A to distribute budget to the distributor 106. A response to the distributor 106 granting more budget (or denying more budget) might be sent immediately as a response to the request communication 1482AB, or it might be sent at a later time as part of a separate communication. The response communication, upon being received at the distributor's VDE node 106, might be processed using the reply process 1475B within the distributor's copy of the BUDGET method 1510B. The reply process 1475B might then process the additional budget in the same manner as described above.

	Claim Term / Phrase	InterTrust Evidence
		The chain of handling and control may, in addition to posting budget information, also pass control information that governs the manner in which said budget may be utilized. For example, the control information specified in the above example may also contain control information describing the process and limits that apply to the distributor's redistribution of the right to use the creator's content object. Thus, when the distributor responds to a budget request from a user (a communication between a user at VDE node 112 to the distributor at VDE node 106 similar in nature to the one described above between VDE nodes 106 and 102) using the distribute process 1472B within the distributor's copy of the BUDGET method 1510B, a distribution and request/response/reply process similar to the one described above might be initiated. '193 patent at 172:61-174:29.
		3(D) BILLING method 406 may then pass the event on to a BUDGET method 408. BUDGET method 408 sets limits and records transactional information associated with those limits. For example, BUDGET method 408 may store budget information in a budget UDE, and may store an audit record in a budget trail UDE. BUDGET method 408 may result in a "budget remaining" field in a budget UDE being decremented by an amount specified by BILLING method 406. '193 patent at 182:22-30.
		3(E) BUDGET method 1510 may read and update budget information within a BUDGET method UDE, '193 patent at 184:67-185:1.
		3(F) Figure 5A shows how the virtual distribution environment 100, in a preferred embodiment, may package information elements (content) into a "container" 302 so the information can't be accessed except as

	Claim Term / Phrase	InterTrust Evidence
		provided by its "rules and controls." Normally, the container 302 is electronic rather than physical. Electronic container 302 in one example comprises "digital" information having a well defined structure. Container 302 and its contents can be called an "object 300." The Figure 5A example shows items "within" and enclosed by container 302. However, container 302 may "contain" items without those items actually being stored within the container. For example, the container 302 may reference items that are available elsewhere such as in other containers at remote sites. Container 302 may reference items available at different times or only during limited times. Some items may be too large to store within container 302. Items may, for example, be delivered to the user in the form of a "live feed" of video at a certain time. Even then, the container 302 "contains" the live feed (by reference) in this example. Container 302 may contain information content 304 in electronic (such as "digital") form. Information content 304 could be the text of a novel, a picture, sound such as a musical performance or a reading, a movie or other video, computer software, or just about any other kind of electronic information you can think of. Other types of "objects" 300 (such as "administrative objects") may contain "administrative" or other information instead of or in addition to information content 304. In the Figure 5A example, container 302 may also contain "rules and controls" in the form of: (a) a "permissions record" 808; (b) "budgets" 308; and (c) "other methods" 1000. Figure 5B gives some additional detail about permissions record 808, budgets 308 and other methods 1000. The "permissions record" 808 specifies the rights associated with the object 300 such as, for example, who can open the container 302, who can use the object's contents, who can distribute the object, and what other control mechanisms must be active. For example, permissions record 808 may specify a user's rights to use, distribute and/or administer the container 302 and its content. Permissions record 808 may also specify requirements to be applied by the budgets 308 and "other methods" 1000. Permissions record 808 may also contain security related information such as scrambling and descrambling "keys."

	Claim Term / Phrase	InterTrust Evidence

> "Budgets" 308 shown in Figure 5B are a special type of "method" 1000 that may specify, among other things, limitations on usage of information content 304, and how usage will be paid for. Budgets 308 can specify, for example, how much of the total information content 304 can be used and/or copied. The methods 310 may prevent use of more than the amount specified by a specific budget.
>
> "Other methods" 1000 define basic operations used by "rules and controls." Such "methods" 1000 may include, for example, how usage is to be "metered," if and how content 304 and other information is to be scrambled and descrambled, and other processes associated with handling and controlling information content 304. For example, methods 1000 may record the identity of anyone who opens the electronic container 302, and can also control how information content is to be charged based on "metering." Methods 1000 may apply to one or several different information contents 304 and associated containers 302, as well as to all or specific portions of information content 304.

'193 patent at 58:38-59:37.

3(G)

> FIGURES 5A and 5B show an example of an "object";

'193 patent at 50:18.

3(H)

Field type	Format	Typical Use	Description or Use
Ascending Use Counter	byte, short, long, or unsigned versions of the same widths	Meter/ Budget	Ascending count of uses.
Descending Use Counter	byte, short, long, or unsigned	Budget	Descending count of permitted use, e.g., remaining

	Claim Term / Phrase	InterTrust Evidence
		versions of the same widths budget: '193 patent at 143:57-65. **3(I)** As with standard VDE objects 300, a user may be required to contact a clearinghouse service to acquire additional budgets if the user wishes to continue to use the traveling object after the exhaustion of an available budget(s) . . . . '193 patent at 131:10-13. **3(J)** Once the distributor 106 has used some or all of her budget, she may desire to obtain additional budget. The distributor 106 might then initiate a process using the BUDGET method request process (1480B). Request process 1480B might initiate a communication (1482AB) with the content creator VDE node 102 requesting more budget and perhaps providing details of the use activity to date (e.g., audit trails). The content creator 102 processes the 'get more budget' request event 1482AB using the response process (1484A) within the creator's BUDGET method 1510A. Response process 1484A might, for example, make a determination if the use information indicates proper use of the content, and/or if the distributor is credit worthy for more budget. The BUDGET method response process 1484A might also initiate a financial transaction to transfer funds from the distributor to pay for said use, or use the distribute process 1472A to distribute budget to the distributor 106. A response to the distributor 106 granting more budget (or denying more budget) might be sent immediately as a response to the request communication 1482AB, or it might be sent at a later time as part of a separate communication. The response communication, upon being received at the distributor's VDE node 106, might be processed using the reply process 1475B within the distributor's copy of the BUDGET method 1510B. The reply process 1475B might then process the additional budget in the same manner as described above. '193 patent at 173:21-174:14.

	Claim Term / Phrase	InterTrust Evidence
		3(K) During the same or different communications exchange, the same or different clearinghouse may handle the end user's request for additional budget and/or permission pertaining to VDE object 300. For example, the end user's electronic appliance 600 may (e.g., in response to a user input request to access a particular VDE object 300) send an administrative object to the clearinghouse requesting budgets and/or other permissions allowing access (Block 1164). As mentioned above, such requests may be transmitted in the form of one or more administrative objects, such as, for example, a single administrative object having multiple "events" associated with multiple requested budgets and/or other permissions for the same or different VDE objects 300. The clearinghouse may upon receipt of such a request, check the end user's credit, financial records, business agreements and/or audit histories to determine whether the requested budgets and/or permissions should be given. The clearinghouse may, based on this analysis, send one or more responsive administrative objects which cause the end user's electronic appliance 600 to update its secure database in response (Block 1166, 1168). This updating might, for example, comprise replacing an expired PERC 808 with a fresh one, modifying a PERC to provide additional (or lesser) rights, etc. Steps 1164-1168 may be repeated multiple times in the same or different communications session to provide further updates to the end user's secure database 610. '193 patent at 162:39-65.
		<u>**Extrinsic Sources**</u> 3(L) **budget** *n.* **1.a.** An itemized summary of estimated or intended expenditures for a given period along with proposals for financing them: *submitted the annual budget to Congress.* **b.** A systematic plan for the expenditure of a usually fixed resource, such as money or time, during a given period: *A new car will not be part of our budget this year.* **c.** The total sum of money allocated for a particular purpose or period of time: *a project with an annual budget of five million dollars.* **2.** A stock or collection with definite limits: "*his budget of general knowledge.*" (William Hazlitt). – **budget** *v.* **—et-ed, et-ing, -ets.** *–tr.* **1.** To plan in advance the expenditure of: *needed help budgeting our income; budgeted my time wisely.* **2.** To enter or account for in a budget: *forgot to budget*

	Claim Term / Phrase	InterTrust Evidence
		the car payments. *–intr.* To make or use a budget. **–budget** *adj.* **1.** Of or relating to a budget: *budget items approved by Congress.* **2.** Appropriate to a budget; inexpensive: *a budget car; budget meals.* American Heritage Dictionary, 3d ed. (Houghton Mifflin, 1992), p. 249.

	Claim Term / Phrase	InterTrust Evidence
4.	clearinghouse 193.19	**Patent Specifications** **4(A)** Clearinghouses may provide independent financial services, such as credit and/or billing services, and can serve as distributors and/or creators. '193 patent at 267:40-42. **4(B)** if appropriate credit (e.g. an electronic clearinghouse account from a clearinghouse such as VISA or AT&T) is available. '193 patent at 25:22-24. **4(C)** clearinghouses that gather usage information regarding, and bill for the use of, electronic information. '193 patent at 3:32-33. **4(D)** in certain models, a clearinghouse might also serve as a rights distribution agent who provides one or more rights to certain value chain participants, which one or more rights may be "attached" to one or more rights to use the clearinghouse's credit (if said clearinghouse is, at least in part, a financial clearinghouse (such a control information provider may alternatively, or in addition, restrict other users' rights. '193 patent at 269:59-65. **4(E)** A document may have an attribute requiring that each use of the document be reported to a central document tracking clearinghouse. This could be used by the organization to track specific documents,

	Claim Term / Phrase	InterTrust Evidence
		to identify documents used by any particular user and/or group of users to track documents with specific attributes (e.g., sensitivity), etc. '193 patent at 280:18-24. **4(F)** In this Figure 2 example, information relating to content use is, as shown by arrow 114, reported to a financial clearinghouse 116. Based on this "reporting," the financial clearinghouse 116 may generate a bill and send it to the content user 112 over a "reports and payments" network 118. Arrow 120 shows the content user 112 providing payments for content usage to the financial clearinghouse 116. Based on the reports and payments it receives, the financial clearinghouse 116 may provide reports and/or payments to the distributor 106. '193 patent at 55:57-66. **4(G)** The "financial clearinghouse" 116 shown in Figure 2 may also be a "VDE administrator." Financial clearinghouse 116 in its VDE administrator role sends "administrative" information to the VDE participants. This administrative information helps to keep the virtual distribution environment 100 operating properly. The "VDE administrator" and financial clearinghouse roles may be performed by different people or companies, and there can be more than one of each. '193 patent at 56:16-24. **4(H)** A summary of the roles of the various participants of virtual distribution environment 100 is set forth in the table below: Role — Description "Traditional" Participants Content creator — Packager and initial distributor of digital

	Claim Term / Phrase	InterTrust Evidence
		information Content Owner — Owner of the digital information. Distributors — Provide rights distribution services for budgets and/or content. Auditor — Provides services for processing and reducing usage based audit trails. Clearinghouse — Provides intermediate store and forward services for content and audit information. Also, typically provides a platform for other services, including third party financial providers and auditors. '193 patent at 255:33-51. 4(I) Further Chain of Handling Model As described in connection with Figure 2, there are four (4) "participant" instances of VDE 100 in one example of a VDE chain of handling and control used, for example, for content distribution. '193 patent at 253:64-254:1. 4(J) FIGURE 2 illustrates an example of a chain of handling and control; '193 patent at 50:8-9. 4(K) a "trusted" financial clearinghouse (e.g., VISA, Mastercard). '193 patent at 41:8-9.

	Claim Term / Phrase	InterTrust Evidence
5.	compares 900.155	**Patent Specifications** **5(A)** Comparing Figure 50 with Figure 49 reveals that the same overall high level processing may typically be performed for READ method 1650 as was described in connection with OPEN method 1500. '900 patent at 195:9-12. **5(B)** As compared to Figure 2, Figure 77 includes a new "client administrator" participant 700. '900 patent at 280:63-65. **5(C)** VDE content, and the electronic agreements associated with said content, can be employed and progressively manipulated in commercial ways which reflect traditional business practices for non-electronic products (though VDE supports greater flexibility and efficiency compared with most of such traditional models). '900 patent at 322:15-20. **Extrinsic Sources** **5(D)** **compare** *v. tr.* **1.** To consider or describe as similar, equal, or analogous; liken. **2.** *Abbr.* **cp.** To examine in order to note the similarities or differences of. **3.** *Grammar.* To form the positive, comparative, or superlative degree of (an adjective or adverb). – *intr.* **1.** To be worthy of comparison; bear comparison: *two concert halls that just do not compare.* **2.** To draw comparisons. **comparison** *n.* **1.a.** The act of comparing or the process of being compared. American Heritage Dictionary, 3d ed. (Houghton Mifflin, 1992), p. 384.

	Claim Term / Phrase	InterTrust Evidence
6.	**component assembly** 912.8, 912.35	**<u>Patent Specifications</u>** **6(A)** ROS VDE functions 604 may be based on segmented, independently loadable executable "component assemblies" 690. These component assemblies 690 are independently securely deliverable. The component assemblies 690 provided by the preferred embodiment comprise code and data elements that are themselves independently deliverable. Thus, each component assembly 690 provided by the preferred embodiment is comprised of independently securely deliverable elements which may be communicated using VDE secure communication techniques, between VDE secure subsystems. These component assemblies 690 are the basic functional unit provided by ROS 602. The component assemblies 690 are executed to perform operating system or application tasks. '193 patent at 83:12-26. --- **6(B)** Components 690 are preferably designed to be easily separable and individually loadable. ROS 602 assembles these elements together into an executable component assembly 690 prior to loading and executing the component assembly (e.g., in a secure operating environment such as SPE 503 and/or HPE 655). '193 patent at 83:43-48. --- **6(C)** Thus, the channel 594 is the mechanism in the preferred embodiment that collects together or assembles the elements shown in Figure 11E into a component assembly 690 that may be used for event processing. '193 patent at 115:67-116:4. ---

	Claim Term / Phrase	InterTrust Evidence
		6(D) In the preferred embodiment, ROS 602 assembles component assemblies 690 based on the following types of elements: Permissions Records ("PERC"s) 808; Method "Cores" 1000; Load Modules 1100; Data Elements (e.g., User Data Elements ("UDEs") 1200 and Method Data Elements ("MDEs") 1202); and Other component assemblies 690. '193 patent at 85:21-29.
		6(E) The selected method event record 1012, in turn, specifies the appropriate information (e.g., load module(s) 1100, data element UDE(s) and MDE(s) 1200, 1202, and/or PERC(s) 808) used to construct a component assembly 690 for execution in response to the event that has occurred. '193 patent at 138:31-36.
		6(F) The reciprocal process 1454 may be based on a component assembly 690 (e.g., one or more load modules 1100, data, and optionally other methods present in the VDE node 600B). '193 patent at 171:39-42.
		6(G) One important security layer involves ensuring that certain component assemblies 690 are formed, loaded and executed only in secure execution space such as provided within an SPU 500. '193 patent at 87:35-38.

	Claim Term / Phrase	InterTrust Evidence
		6(H) ROS 602 provided by the preferred embodiment responds to an event by specifying and beginning processes to process the event. These processes are, in the preferred embodiment, based on methods 1000. Since there are an unlimited number of different types of events, the preferred embodiment supports an unlimited number of different processes to process events. This flexibility is supported by the dynamic creation of component assemblies 690 from independently deliverable modules such as method cores 1000', load modules 1100, and data structures such as UDEs 1200. '193 patent at 169:62-170:4.
		6(I) In the preferred embodiment, ROS 602 assembles securely independently deliverable elements into a component assembly 690 based in part on context parameters (e.g., object, user). '193 patent at 84:17-20.
		6(J) This "channel 0" "open channel" task may then issue a series of requests to secure database manager 566 to obtain the "blueprint" for constructing one or more component assemblies 690 to be associated with channel 594 (block 1127). In the preferred embodiment, this "blueprint" may comprise a PERC 808 and/or URT 464. . . . The preferred embodiment process may next use the "blueprint" to access (e.g, the secure database manager 566 and/or from load module execution manager library(ies) 568) the appropriate "control method" that may be used to, in effect, supervise execution of all of the other methods 1000 within the channel 594 (block 1131). '193 patent at 112:46-51, 112:63-113:2.

	Claim Term / Phrase	InterTrust Evidence
		<u>File Histories</u> **6(K)** Column 1, lines 33-65 [of Fischer 5,748,960] describes "data types" or "classes" in object-oriented programming that meets the term 'component' recited in the instant claims (i.e. code and data elements that are independently deliverable). '912 Patent File History, 9/22/98 Office Action, pp. 2-3.

	Claim Term / Phrase	InterTrust Evidence
7.	**contain** 683.2, 912.8, 912.35	**<u>Patent Specifications</u>** **7(A)** A VDE content container is an object that contains both content (for example, commercially distributed electronic information products such as computer software programs, movies, electronic publications or reference materials, etc.) and certain control information related to the use of the object's content. '193 patent at 19:15-21. **7(B)** The Figure 5A example shows items "within" and enclosed by container 302. However, container 302 may "contain" items without those items actually being stored within the container. For example, the container 302 may reference items that are available elsewhere such as in other containers at remote sites. Container 302 may reference items available at different times or only during limited times. Some items may be too large to store within container 302. Items may, for example, be delivered to the user in the form of a "live feed" of video at a certain time. Even then, the container 302 "contains" the live feed (by reference) in this example. '193 patent at 58:48-58. **<u>Extrinsic Sources</u>** **7(C)** **contain** *tr.v.* **-tained, -tain-ing, -tains. 1. a.** To have within; hold. **b.** To be capable of holding. **2.** To have as component parts; include or comprise: *The album contains many memorable songs.* **3. a.** To hold or keep within limits; restrain: *I could hardly contain my curiosity.* **b.** To halt the spread or development of; check: *Science sought an effective method of containing the disease.* **4.** To check the expansion or influence of (a hostile power or ideology) by containment. **5.** *Mathematics*. To be exactly divisible by.[Middle English *conteinen*, from Old French *contenir*, from Latin *continere* : *com-*, com- + *tenere*, to hold. See ten-.]**--con-tain'a-ble** *adj.*

	Claim Term / Phrase	InterTrust Evidence
		SYNONYM: contain, hold, accommodate. These verbs mean to have within or have the capacity for having within. *Contain* means to have within or have as a part or constituent: *This drawer contains all the cutlery we own. The book contains some amusing passages. Polluted water contains contaminants. Hold* can be used in that sense but primarily stresses capacity for containing: *The pitcher holds two pints but contains only one. Accommodate* refers to capacity for holding comfortably: *The restaurant accommodates 50 customers. Four hundred inmates were crowded into a prison intended to accommodate 200* . American Heritage Dictionary, 3d ed. (Houghton Mifflin, 1992), p. 406.

	Claim Term / Phrase	InterTrust Evidence
8.	**control (n.)** 193.1, 193.11, 193.15, 193.19, 891.1	**<u>Patent Specifications</u>** **8(A)** Consumers 206, 208, 210 are each capable of receiving and using the programs created by video production studio 204—assuming, that is, that the video production studio or information utility 200 has arranged for these consumers to have appropriate "rules and controls" (control information) that give the consumers rights to use the programs. '193 patent at 53:53-59. **8(B)** The virtual distribution environment 100 prevents use of protected information except as permitted by the "rules and controls" (control information). For example, the "rules and controls" shown in Figure 2 may grant specific individuals or classes of content users 112 "permission" to use certain content. They may specify what kinds of content usage are permitted, and what kinds are not. They may specify how content usage is to be paid for and how much it costs. As another example, "rules and controls" may require content usage information to be reported back to the distributor 106 and/or content creator 102. '193 patent at 56:26-36. **8(C)** Objects may be classified in one sense based on whether the protection information is bound together with the protected information. For example, a container that is bound by its control(s) to a specific VDE node is called a "stationary object" (see Figure 18). A container that is not bound by its control information to a specific VDE node but rather carries sufficient control and permissions to permit its use, in whole or in part, at any of several sites is called a "Traveling Object".... '193 patent at 129:52-60.

	Claim Term / Phrase	InterTrust Evidence

8(D)

> VDEF load modules, associated data, and methods form a body of information that for the purposes of the present invention are called "control information." VDEF control information may be specifically associated with one or more pieces of electronic content and/or it may be employed as a general component of the operating system capabilities of a VDE installation.

'193 patent at 18:36-42.

8(E)

> Failure information, including the elements listed below, may be saved along with details of the failure:
>
> | Control Information Retained in an SPE on Access Failures |
> |---|
> | Object ID |
> | User ID |
> | Type of failure |
> | Time of failure |
>
> This information may be analyzed to detect cracking attempts or to determine patterns of usage outside expected (and budgeted) norms. The audit trail histories in the SPU 500 may be retained until the audit is reported to the appropriate parties.

'193 patent at 121:15-32.

8(F)

> In this embodiment, the additional memory may be provided by additional one or more integrated circuits that can be contained within a secure enclosure, such as a tamper resistant metal container or some form of a chip pack containing multiple integrated circuit components, and which impedes and/or evidences tampering attempts, and/or disables a portion or all of SPU 500 or associated critical key and/or other control information in the event of tampering.

'193 patent at 169:5-13.

	Claim Term / Phrase	InterTrust Evidence
		8(G) . . . may involve preserving at least a portion of the control information (e.g., executable code such as load modules) '193 patent at 33:12-14.
		8(H) VDE control information may, in part or in full, (a) represent control information directly put in place by VDE content control information pathway participants, and/or (b) comprise control information put in place by such a participant on behalf of a party who does not directly handle electronic content (or electronic appliance) permissions records information (for example control information inserted by a participant on behalf of a financial clearinghouse or government agency). Such control information methods (and/or load modules and/or mediating data and/or component assemblies) may also be put in place by either an electronic automated, or a semi-automated and human assisted, control information (control set) negotiating process that assesses whether the use of one or more pieces of submitted control information will be integrated into and/or replace existing control information (and/or chooses between alternative control information based upon interaction with in-place control information) and how such control information may be used. '193 patent at 44:34-52.
		8(I) In either embodiment, certain control information (software and parameter data) must be securely maintained within the SPU, and further control information can be stored externally and securely (e.g. in encrypted and tagged form) and loaded into said hardware SPU when needed. '193 patent at 49:50-55.
		8(J) Content control information governs content usage according to

	Claim Term / Phrase	InterTrust Evidence
		criteria set by holders of rights to an object's contents and/or according to parties who otherwise have rights associated with distributing such content (such as governments, financial credit providers, and users). '193 patent at 15:46-50. **8(K)** VDE's usage control information, for example, provide for property content and/or appliance related: usage authorization, usage auditing (which may include audit reduction), usage billing, usage payment, privacy filtering, reporting, and security related communication and encryption techniques. '193 patent at 15:33-38. **8(L)** Control information delivered by, and/or otherwise available for use with, VDE content containers comprise (for commercial content distribution purposes) VDEF control capabilities (and any associated parameter data) for electronic content. These capabilities may constitute one or more "proposed" electronic agreements (and/or agreement functions available for selection and/or use with parameter data) that manage the use and/or the consequences of use of such content and which can enact the terms and conditions of agreements involving multiple parties and their various rights and obligations. '193 patent at 19:22-32. **8(M)** . . . an end-user of such content might be limited by the same content control information to making three copies of such content, one for each of three different computers he or she uses (one desktop computer at work, one for a desktop computer at home, and one for a portable computer). '193 patent at 48:29-34.

	Claim Term / Phrase	InterTrust Evidence
		8(N) In the Figure 5A example, container 302 may also contain "rules and controls" in the form of: (a) a "permissions record" 808; (b) "budgets" 308; and (c) "other methods" 1000. Figure 5B gives some additional detail about permissions record 808, budgets 308 and other methods 1000. The "permissions record" 808 specifies the rights associated with the object 300 such as, for example, who can open the container 302, who can use the object's contents, who can distribute the object, and what other control mechanisms must be active. For example, permissions record 808 may specify a user's rights to use, distribute and/or administer the container 302 and its content. Permissions record 808 may also specify requirements to be applied by the budgets 308 and "other methods" 1000. Permissions record 808 may also contain security related information such as scrambling and descrambling "keys." "Budgets" 308 shown in Figure 5B are a special type of "method" 1000 that may specify, among other things, limitations on usage of information content 304, and how usage will be paid for. Budgets 308 can specify, for example, how much of the total information content 304 can be used and/or copied. The methods 310 may prevent use of more than the amount specified by a specific budget. '193 patent at 59:1-25.
		8(O) A distributed database may manage such a distributed repository resource environment and use VDE to secure the storing, communicating, auditing, and/or use of information through VDE's electronic enforcement of VDE controls. '193 patent at 284:22-26.
		8(P) ROS 602 provided by the preferred embodiment extends

	Claim Term / Phrase	InterTrust Evidence
		conventional capabilities such as, for example, Access Control List (ACL) structures, to user and process defined events, including state transitions. ROS 602 may provide full control information over pre-defined and user-defined application events. These control mechanisms include "go/no-go" permissions, and also include optional event-specific executables that permit complete flexibility in the processing and/or controlling of events. This structure permits events to be individually controlled so that, for example, metering and budgeting may be provided using independent executables. For example, ROS 602 extends ACL structures to control arbitrary granularity of information. Traditional operating systems provide static "go-no go" control mechanisms at a file or resource level; ROS 602 extends the control concept in a general way from the largest to the smallest sub-element using a flexible control structure. ROS 602 can, for example, control the printing of a single paragraph out of a document file. '193 patent at 77:45-63. **8(Q)** ROS 602 provided by the preferred embodiment permits secure modification and update of control information governing each component. The control information may be provided in a template format such as method options to an end-user. An end-user may then customize the actual control information used within guidelines provided by a distributor or content creator. '193 patent at 77:64-78:3. **8(R)** VDE control information (e.g., methods) that collectively control use of VDE managed properties (database, document, individual commercial product), are either shipped with the content itself (for example, in a content container) and/or one or more portions of such control information is shipped to distributors and/or other users in separably deliverable "administrative objects." A subset of the methods for a property may in part be delivered with each property while one or more other subsets of methods can be delivered

	Claim Term / Phrase	InterTrust Evidence
		separately to a user or otherwise made available for use (such as being available remotely by telecommunication means). '193 patent at 43:26-37. **8(S)** Many such load modules are inherently configurable, aggregatable, portable, and extensible and singularly, or in combination (along with associated data), run as control methods under the VDE transaction operating environment. '193 patent at 25:48-52. **8(T)** Traveling objects can be used at a receiving VDE node electronic appliance 600 so long as either the appliance carries the correct budget or budget type (e.g. sufficient credit available from a clearinghouse such as a VISA budget) either in general or for specific one or more users or user classes, or so long as the traveling object itself carries with it sufficient budget allowance or an appropriate authorization (e.g., a stipulation that the traveling object may be used on certain one or more installations or installation classes or users or user classes where classes correspond to a specific subset of installations or users who are represented by a predefined class identifiers stored in a secure database 610). After receiving a traveling object, if the user (and/or installation) doesn't have the appropriate budget(s) and/or authorizations, then the user could be informed by the electronic appliance 600 (using information stored in the traveling object) as to which one or more parties the user could contact. '193 patent at 131:33-50. **8(U)** [A]n object provider might allow users to redistribute copies of an object to their friends and associates (for example by physical delivery of storage media or by delivery over a computer network) such that if a friend or associate satisfies any certain criteria required for use of said object, he may do so.

	Claim Term / Phrase	InterTrust Evidence
		For example, if a software program was distributed as a traveling object, a user of the program who wished to supply it or a usable copy of it to a friend would normally be free to do so. Traveling Objects have great potential commercial significance, since useful content could be primarily distributed by users and through bulletin boards, which would require little or no distribution overhead apart from registration with the "original" content provider and/or clearinghouse. The "out of channel" distribution may also allow the provider to receive payment for usage and/or elsewise maintain at least a degree of control over the redistributed object. Such certain criteria might involve, for example, the registered presence at a user's VDE node of an authorized third party financial relationship, such as a credit card, along with sufficient available credit for said usage. Thus, if the user had a VDE node, the user might be able to use the traveling object if he had an appropriate, available budget available on his VDE node (and if necessary, allocated to him), and/or if he or his VDE node belonged to a specially authorized group of users or installations and/or if the traveling object carried its own budget(s). '193 patent at 131:59-132:18. **8(V)** VDE supports multiple differing hierarchies of client organization control information wherein an organization client administrator distributes control information specifying the usage rights of departments, users, and/or projects. Likewise, a department (division) network manager can function as a distributor (budgets, access rights, etc.) for department networks, projects, and/or users, etc. '193 patent at 33:63-34:3. **<u>File Histories</u>** **8(W)** Claims . . . are rejected under 35 U.S.C. 102(b) as being anticipated by Lofberg (4,595,950).

	Claim Term / Phrase	InterTrust Evidence
		The recited first device and its operation matches that of the rent terminal. . . . The information including at least one control is the personal identification information, see col. 3, lines 60-68 and col. 4, lines 64-68 and col. 13, lines 1-11. . . . The second device is the user station. The rent terminal determines whether the digital file may be copied and stored on the second device, see col. 9, lines 1-8 and col. 12, lines 43-49. The second device renders the digital file through its output only upon the data carrier having the information recorded therein and governing the use of the digital file is transferred to the second device. '193 Patent File History, 6/7/00 Office Action, p. 2. **8(X)** Claims . . . are rejected . . . as being anticipated by Karp (4,866,769). . . . The first device is a personal computer that is allowed access to the software by virtue of an encoded checkword derived from a source ID on the diskette and the personal computer ID, see Abstract. The information including at least one control is the list of checkwords stored in association with the digital file, see col. 5, line 60 through col. 6, line 11. A second device is represented by a second checkword stored in the list, see col. 8, lines 1-18. The determination of whether the digital file may be copied and stored by a second device is dependent on whether a checkword for the second device is allowed. '193 Patent File History, 6/7/00 Office Action, pp. 3-4. **8(Y)** Claims 58-59 are rejected . . . as being anticipated by Schull [5,509,070]. The Schull reference describes a system for distribution, registration and purchase of software. . . The identified control is the need for a valid password to unlock the advanced features of the copied

	Claim Term / Phrase	InterTrust Evidence
		software. Column 7, line 10 through column 8, line 9 describe the generation and assignment of the target IDs and passwords. USP 5,915,019 File History, 7/28/97 Office Action, p. 3. **8(Z)** [Okano, 5,504,818] describes a system using cryptography for processing various digital objects. Figure 3 and column 6, line 33 disclose where a protected object may have embedded additional elements (security code attributes) to associate a control on the object. The control would restrict information according to security levels. USP 5,915,019 File History, 7/28/97 Office Action, p. 3. **8(AA)** A comparison of independent claim 7 to Fischer to derive the similarities and differences between the claimed invention and the prior art follows. Figure 1 of Fischer shows various terminals connected via a communications channel 12. Terminal A, as a first apparatus recited in claim 7, includes user controls as per keyboard / crt 4; communications port, see modem and communications channel 12; a processor as processor with main memory, 2.... '683 File History, 11/12/99 Office Action, p. 4.

	Claim Term / Phrase	InterTrust Evidence
9.	**controlling, control (v.)** 193.1, 861.58	**Patent Specifications** **9(A)** Secondary storage 652 in this example stores code and data used by CPU 654 and/or SPU 500 to control the overall operation of electronic appliance 600. '193 patent at 62:58-60. **9(B)** The other CPU(s) 654 may be any centrally controlling logic arrangement, such as for example, a microprocessor, other microcontroller, and/or array or other parallel processor. '193 patent at 64:55-58. **9(C)** A shared address/data bus arrangement 536 may transfer information between these various components under control of microprocessor 520 and/or DMA controller 526. '193 patent at 65:35-38. **9(D)** In some implementations, a separate arithmetic accelerator 544 may be omitted and any necessary calculations may be performed by microprocessor 520 under software control. '193 patent at 68:46-49. **9(E)** DMA controller 526 controls information transfers over address/data bus 536 without requiring microprocessor 520 to process each individual data transfer. '193 patent at 68:51-53.

	Claim Term / Phrase	InterTrust Evidence
		9(F) In the preferred embodiment, to control access to clearinghouses, users are assigned account numbers at clearinghouses. '193 patent at 268:29-31.
		9(G) . . . plural, different control models regulating the use and/or auditing of either the same specific copy of electronic information content and/or differently regulating different copies (occurrences) of the same electronic information content. Differing models for billing, auditing, and security can be applied to the same piece of electronic information content and such differing sets of control information may employ, for control purposes, the same, or differing, granularities of electronic information control increments. This includes supporting variable control information for budgeting and auditing usage as applied to a variety of predefined increments of electronic information, including employing a variety of different budgets and/or metering increments for a given electronic information deliverable for: billing units of measure, credit limit, security budget limit and security content metering increments, and/or market surveying and customer profiling content metering increments. '193 patent at 28:19-37.
		9(H) . . . support the flowing of content control information through different "branches" of content control information handling so as to accommodate, under the present invention's preferred embodiment, diverse controlled distributions of VDE controlled content. This allows different parties to employ the same initial electronic content with differing (perhaps competitive) control strategies. In this instance, a party who first placed control information on content can make certain control assumptions and these assumptions would evolve into more specific and/or extensive control assumptions. These control assumptions can evolve during the branching sequence upon content model participants submitting control information changes, for example, for use in "negotiating" with "in place" content control information. This can result in new or

	Claim Term / Phrase	InterTrust Evidence
		modified content control information and/or it might involve the selection of certain one or more already "in-place" content usage control methods over in-place alternative methods, as well as the submission of relevant control information parameter data. This form of evolution of different control information sets applied to different copies of the same electronic property content and/or appliance results from VDE control information flowing "down" through different branches in an overall pathway of handling and control and being modified differently as it diverges down these different pathway branches. '193 patent at 31:29-56.
		9(I) . . . multiple simultaneous control models for the same content property and/or property portion. This allows, for example, for concurrent business activities which are dependent on electronic commercial product content distribution, such as acquiring detailed market survey information and/or supporting advertising, both of which can increase revenue and result in lower content costs to users and greater value to content providers. Such control information and/or overall control models may be applied, as determined or allowed by control information, in differing manners to different participants in a pathway of content, reporting, payment, and/or related control information handling. VDE supports applying different content control information to the same and/or different content and/or appliance usage related activities, and/or to different parties in a content and/or appliance usage model, such that different parties (or classes of VDE users, for example) are subject to differing control information managing their use of electronic information content. For example, differing control models based on the category of a user as a distributor of a VDE controlled content object or an end-user of such content may result in different budgets being applied. Alternatively, for example, a one distributor may have the right to distribute a different array of properties than another distributor (from a common content collection provided, for example, on optical disc). An individual, and/or a class or other grouping of end-users, may have different costs (for example, a student, senior citizen, and/or poor citizen user of content who may be provided with the same or differing discounts) than a "typical" content user. '193 patent at 30:42-31:7.

	Claim Term / Phrase	InterTrust Evidence

9(J)

> Such different application of control information may also result from content control information specifying that a certain party or group of parties shall be subject to content control information that differs from another party or group of parties. For example, content control information for a given piece of content may be stipulated as senior information and therefore not changeable, might be put in place by a content creator and might stipulate that national distributors of a given piece of their content may be permitted to make 100,000 copies per calendar quarter, so long as such copies are provided to bona fide end-users, but may pass only a single copy of such content to a local retailers and the control information limits such a retailer to making no more than 1,000 copies per month for retail sales to end-users. In addition, for example, an end-user of such content might be limited by the same content control information to making three copies of such content, one for each of three different computers he or she uses (one desktop computer at work, one for a desktop computer at home, and one for a portable computer).

'193 patent at 48:15-35.

9(K)

> In this example, as illustrated in Figure 80, user B may receive control information associated with creator A's content from distributor A and/or user/distributor B. In either case, user B may be able to establish their own control information on DA(CA) and/or UDB(UDA(DA(CA))), respectively (if allowed by such control information. The resulting set(s) of control information UB(DA(CA)) and/or UB(UDB(UDA(DA(CA)))) respectively, may represent different control scenarios, each of which may have benefits for user B. As described in connection with an earlier example, user B may have received control information from user/distributor B along a chain of handling including user/distributor A that bases fees on the number of minutes that user B makes use of creator A's content (and requiring user/distributor A to pay fees of $15 per month per user to distributor A regardless of the amount of usage by user B in a calendar month). This may be more favorable under some circumstances than the fees required by a direct use of control information provided by distributor A, but may also have the disadvantage of an exhausted chain of redistribution and, for example, further usage information reporting requirements included in UDB(UDA(DA(CA))). If the two sets of

	Claim Term / Phrase	InterTrust Evidence
		control information DA(CA) and UDB(UDA(DA(CA))) permit (e.g. do not require exclusivity enforced, for example, by using a registration interval in an object registry used by a secure subsystem of user B's VDE installation to prevent deregistration and reregistration of different sets of control information related to a certain container (or registration of plural copies of the same content having different control information and/or being supplied by different content providers) within a particular interval of time as an aspect of an extended agreement for a chain of handling and control reflected in DA(CA) and/or UDB(UDA(DA(CA)))), user B may have both sets of control information registered and may make use of the set that they find preferable under a given usage scenario. '193 patent at 306:30-65. **9(L)** For example, user/distributor A may receive control information CB that includes a requirement that user/distributor A pay creator B for content decrypted by user/distributor A (and any participant receiving distributed and/or redistributed control information from user/distributor A) at the rate of $0.50 per kilobyte. As indicated above, user/distributor A also may receive control information associated with creator B's VDE content container from distributor A. In this example, user/distributor A may have a choice between paying a "rental" fee through a chain of handling passing through distributor A, and a fee based on the quantity of decryption through a chain of handling direct to creator B. In this case, user/distributor A may have the ability to choose to use either or both of CB and DA(CB). '193 patent at 308:29-42. **9(M)** As illustrated in Figure 81, in this example, user B may receive control information associated with creator B's VDE content container from six different sources: CB directly from creator B, DA(CB) from distributor A, UDB(UDA(DA(CB))) and/or UDB(UDA(CB)) from user/distributor B, DC(CB) from distributor C, and/or DB(DC(CB)) from distributor B. This represents six chains of handling through which user B may enter into extended agreements with other participants in this example. Two of these

	Claim Term / Phrase	InterTrust Evidence
		chains pass through user/distributor B. Based on a VDE negotiation between user/distributor B and user B, an extended agreement may be reached (if permitted by control information governing both parties) that reflects the conditions under which user B may use one or both sets of control information. In this example, two chains of handling and control may "converge" at user/distributor B, and then pass to user B (and if control information permits, later diverge once again based on distribution and/or redistribution by user B). '193 patent at 308:48-65. --- **9(N)** User B may, in this example, receive a VDE content container from distributor C that is comprised of VDE objects created by creator B, creator C, and creator D. In addition, user B may receive a VDE content container from distributor B that contains the same content created by creator B, creator C, and creator D in addition to one or more extracted/embedded portions of content created by creator E. User B may base decisions concerning which of such containers they choose to use (including which embedded containers she may wish to use), and under which circumstances, based on, for example, the character of such extracted/embedded portions (e.g. multimedia presentations illustrating potential areas of interest in the remainder of the content, commentary explaining and/or expositing other elements of content, related works, improved application software delivered as an element of content, etc.); the quality, utility, and/or price (or other attributes of control information) of such portions; and other considerations which distinguish the containers and/or content control information received, in this example, from distributor B and distributor C. '193 patent at 312:11-31. --- **<u>Extrinsic Sources</u>** **9(O)** **control** *tr. v.* **-trolled, -trol-ling, -trols. 1.** To exercise authoritative or dominating influence over; direct. See Synonyms at **conduct**. **2.** To hold in restraint; check: *struggled to control my temper; regulations intended to control prices.* **3. a.** To verify or regulate (a scientific experiment) by conducting a parallel

	Claim Term / Phrase	InterTrust Evidence
		experiment or by comparing with another standard. **b.** To verify (an account, for example) by using a duplicate register for comparison. –**control** *n.* **1.** Authority or ability to manage or direct: *lost control of the skidding car; the leaders in control of the country.* **2.** *Abbr.* **cont., contr. a.** One that controls; a controlling agent, device, or organization. **b.** Often **controls.** An instrument or set of instruments used to operate, regulate, or guide a machine or vehicle. **3.** A restraining device, measure, or limit; a curb: *a control on prices; price controls.* **4. a.** A standard of comparison for checking or verifying the results of an experiment. **b.** An individual or group used as a standard of comparison in a control experiment. **5.** An intelligence agent who supervises or instructs another agent. **6.** A spirit presumed to speak or act through a medium.[Middle English *controllen*, from Anglo-Norman *contreroller*, from Medieval Latin *contrarotulare*, to check by duplicate register, from *contrarotulus*, duplicate register : Latin *contra-*, contra- + Latin *rotulus*, roll, diminutive of *rota*, wheel. See ret-.]--**con-trol'la-bil'i-ty** *n.* **--con-trol'la-ble** *adj.* American Heritage Dictionary, 3d ed. (Houghton Mifflin, 1992), p. 410.

	Claim Term / Phrase	InterTrust Evidence
10.	**copy, copied, copying** 193.1, 193.11, 193.15, 193.19	**<u>Patent Specifications</u>** **10(A)** In some circumstances, a VDE administrator may require that a copy (partial or complete) of the back up files be transmitted to it within an administrative object to check for indications of fraudulent activities by the user. '193 patent at 167:63-67. **10(B)** When a user needs to access a particular VDE object 300, her electronic appliance 600 could issue a request over network 672 to obtain a copy of the object. The "VDE server" could deliver all or a portion of the requested object 300 in response to the request. '193 patent at 226:11-16. **10(C)** Expiration dates cannot be used effectively to prevent substitution of the previous copy of a budget UDE 1200. To secure these frequently updated items, a transaction tag is generated and included in the encrypted item each time that item is updated. '193 patent at 143:14-18. **10(D)** For example, author 3306A may have required that the repository encrypt each copy of shipped content using a different encryption key or keys in order to help maintain greater protection for content (e.g. in case an encryption key was "cracked" or inadvertently disclosed, the "damage" could be limited to the portion(s) of that specific copy of a certain content deliverable). '193 patent at 288:46-52.

	Claim Term / Phrase	InterTrust Evidence
		10(E) electronic testing will allow users to receive a copy (encrypted or unencrypted) of their test results when they leave the test sessions. '193 patent at 319:13-15. **10(F)** transferring at least a portion of said digital file to a second device including a memory and an audio and/or video output, the portion of said digital file transferred to said second device representing a version of said digital file which, when rendered at said second device, provides a level of quality lower than the level of quality provided when said digital file is rendered at said first device; '193 patent at 323:64-324:4. **10(G)** For example, if the audit information received by the clearinghouse is legitimate, then the clearinghouse may send an administrative object to the end user's electronic appliance 600 requesting the electronic appliance to delete and/or compress the audit information that has been transferred. '193 patent at 162:10-15. **10(H)** [A] user (the "originating user") may wish to place an "originator controlled" ("ORCON") restriction on a certain document, such that the document may be transmitted and used only by those specific other users whom he designates (and only in certain, expressly authorized ways). Such a restriction may be flexible if the "distribution list" could be modified after the creation of the document, specifically in the event of someone requesting permission from the originating user to transmit the document outside the original list of authorized recipients. '193 patent at 278:11-21.

	Claim Term / Phrase	InterTrust Evidence
		10(I) Commercial content repository 200g may store content securely such that users may obtain such, when any required conditions are met, content from the repository 200g. The distribution permissions 3502 may, for example, permit commercial content repository 200g to create redistribution permissions and/or usage permissions 3500, 3502 using a VDE protected subsystem within certain restrictions described in content control information received from creator 102 (e.g., not to exceed a certain number of copies, requiring certain payments by commercial content repository 200g to creator 102, requiring recipients of such permissions to meet certain reporting requirements related to content usage information, etc.). Such content control information may be stored at the repository installation and be applied to unencrypted content as it is transmitted from said repository in response to a user request, wherein said content is placed into a VDE container as a step in a secure process of communicating such content to a user. '193 patent at 316:16-37. **10(J)** 37. A method as in claim 36, further comprising: at some point after said transferring step, taking at least one action to render said copy of said first digital file unuseable at said second device; and at said first digital device, removing said encumbrance on said budget, said removal including increasing the number of copies of said first digital file authorized by said budget. '193 patent at 325:32-40. __Extrinsic Sources__ **10(K)** **copy** To reproduce data in a new location or other destination, leaving the source data unchanged, although the physical form of

	Claim Term / Phrase	InterTrust Evidence
		the result may differ from that of the source; for example, to make a duplicate of all the programs or data on a disk, or to copy a graphic screen image to a printer. Spencer, Personal Computer Dictionary (Camelot Publishing, 1995), p. 47. **10(L)** **copy** 1. The material, including text, graphic images, pictures, and artwork, to be assembled for printing. To reproduce part of a document at another location in the document or in another document. Webster's New World Dictionary of Computer Terms, 6th ed. (1997), p. 118. **10(M)** **copy** *n., pl.* **–ies. 1.** An imitation or reproduction of an original; a duplicate: *a copy of a painting; made two copies of the letter.* **2.** One specimen or example of a printed text or picture: *an autographed copy of a novel.* **3.** *Abbr.* **c., C.** Material, such as a manuscript, that is to be set in type. **4.** The words to be printed or spoken in an advertisement. **5.** Suitable source material for journalism: *Celebrities make good copy.* **–copy** *v.* **-ied, -ying, -ies** *–tr.* **1.** To make a reproduction or copy of. **2.** To follow as a model or pattern; imitate. See Synonyms at **imitate.** *–intr.* **1.** To make a copy or copies. **2.** To admit of being copied: *colored ink that does not copy well.* American Heritage Dictionary, 3d ed. (Houghton Mifflin, 1992), p. 416.

	Claim Term / Phrase	InterTrust Evidence
11.	derive 900.155	**<u>Patent Specifications</u>** **11(A)** Whenever CPU/SPU 2650 enters or leaves the "SPU" mode, the transition is performed in such a way that no information contained in the secure memory 532, 534 or derived from it (e.g., stored in registers or a cache memory associated with microprocessor 2652) while in the "SPU" mode can be exposed by microprocessor 2652 operations that occur in the "normal" mode. '900 patent at 75:30-36. **11(B)** In some example implementations, interrupts may be enabled while CPU/SPU 2650 is operating in the "SPU" mode similarly interrupts and returns from interrupts while in the "SPU" mode may allow transitions from "SPU" mode to "normal" mode and back to "SPU" mode without exposing the content of secure memory 532, 534 or the content of registers or other memory associated with microprocessor 2652 that may contain information derived from secure mode operation. '900 patent at 75:41-49. **11(C)** For example, during PPE 650 operation, the internal state of the PPE is constantly being updated. During each interaction with a trusted server, PPE 650 (and the trusted server) may test the internal state of PPE 650 to determine whether it could be derived from the internal state last seen by the trusted server for this particular PPE 650 instance. If it could not, the result may be taken as indicating a replay attack of some sort, and an appropriate action can be taken (see Figure 69L, block 3592, 3594, 3596). '900 patent at 247:4-12. **11(D)** For example, the counter could be repeated hashing (e.g., with

	Claim Term / Phrase	InterTrust Evidence
		MD5) of a value that is stored redundantly in several different locations within the operational materials 3472 and secure database 610 - so that the trusted server could verify that the current value can be derived (e.g., by repeated MD5 applications) from a previous value. '900 patent at 247:20-26. **<u>Extrinsic Sources</u>** **11(E)** **derive**: *v.* **de-rived, de-riv-ing, de-rives.** *v. tr.* **1.** To obtain or receive from a source. **2.** To arrive at by reasoning; deduce or infer: *derive a conclusion from facts.* **3.** To trace the origin or development of (a word). **4.** *Chemistry.* To produce or obtain (a compound) from another substance by chemical reaction.v. intr. To issue from a source; originate. See Synonyms at **stem1**.[Middle English *deriven*, to be derived from, from Old French *deriver*, from Latin *derivare*, to derive, draw off : *de-*, de- + *rivus*, stream. See rei-.]**--de-riv'a-ble** *adj.* **--de-riv'er** *n.* American Heritage Dictionary, 3d ed. (Houghton Mifflin, 1992), p. 504.

	Claim Term / Phrase	InterTrust Evidence
12.	**designating** 721.1	**Patent Specifications** **12(A)** Figures 11A-11C show how a verifying authority can use different digital signatures to designate the same or different load modules as being appropriate for execution by different assurance level electronic appliances; '721 patent at 7:66-8:2. **12(B)** In one of its roles or instances, object submittal manager 774 provides a user interface 774a that allows the user to create an object configuration file 1240 specifying certain characteristics of a VDE object 300 to be created. This user interface 774a may, for example, allow the user to specify that she wants to create an object, allow the user to designate the content the object will contain, and allow the user to specify certain other aspects of the information to be contained within the object (e.g., rules and control information, identifying information, etc.). '193 patent at 103:11-20. **12(C)** Control sets 914 exist in two types in VDE 100: common required control sets which are given designations "control set 0" or "control set for right," and a set of control set options. '193 patent at 150:30-33. **12(D)** The classification attributes may designate the overall level of sensitivity of the document as an element of an ordered set. For example, the set "unclassified," "confidential," "secret," "top secret" might be appropriate in a government setting, and the set "public," "internal," "confidential," "registered confidential" might be appropriate in a corporate setting.

	Claim Term / Phrase	InterTrust Evidence
		The compartment attributes may designate the document's association with one or more specific activities within the organization, such as departmental subdivisions (e.g., "research," "development," "marketing") or specific projects within the organization. Each person using an electronic appliance 600 would be assigned, by an authorized user, a set of permitted sensitivity attributes to designate those documents, or one or more portions of certain document types, which could be processed in certain one or more ways, by the person's electronic appliance. A document's sensitivity attribute would have to belong to the user's set of permitted sensitivity values to be accessible. In addition, the organization may desire to permit users to exercise control over specific documents for which the user has some defined responsibility. As an example, a user (the "originating user") may wish to place an "originator controlled" ("ORCON") restriction on a certain document, such that the document may be transmitted and used only by those specific other users whom he designates (and only in certain, expressly authorized ways). '193 patent at 277:56-278:16.
		12(E) A document may have an attribute designating its originator and requiring an explicit permission to be granted by an originator before the document's content could be viewed. '193 patent at 280:1-4.
		Extrinsic Sources **12(F)** **designate** *tr. v.* **–nated, -nating, -nates. (1)** To indicate or specify; point out. **(2)** To give a name or title to; characterize. **(3)** To select and set aside for a duty, an office, or a purpose. See Synonyms at **allocate, appoint.** American Heritage Dictionary, 3d ed. (Houghton Mifflin, 1992), p. 506.

	Claim Term / Phrase	InterTrust Evidence
13.	**device class** 721.1	**<u>File Histories</u>** **13(A)** . . . Applicants respectfully submit that some of the terms cited by the Examiner as "indefinite" are either well-known by persons skilled in the art or inherently clear. For example . . . the term "class" is used as part of the phrase "device class." Applicants respectfully submit that "device class" is inherently clear, meaning a group of devices which share at least one attribute. '721 Patent File History, 4/13/99 Response, p. 14.

	Claim Term / Phrase	InterTrust Evidence
14.	**digital signature, digitally signing** 721.1	**<u>Patent Specifications</u>** **14(A)** A verifying authority digitally "signs" and "certifies" those load modules or other executables it has verified (using a public key based digital signature and/or certificate based thereon, for example). Protected execution spaces such as protected processing environments can be programmed or otherwise conditioned to accept only those load modules or other executables bearing a digital signature/certificate of an accredited (or particular) verifying authority. '721 patent at 4:64-5:5. --- **14(B)** In accordance with another aspect provided by the present invention, an execution environment protects itself by deciding — based on digital signatures, for example — which load modules or other executables it is willing to execute. A digital signature allows the execution environment to test both the authenticity and the integrity of the load module or other executables, as well permitting a user of such executables to determine their correctness with respect to their associated specifications or other description of their behavior, if such descriptions are included in the verification process. '721 patent at 6:5-15. --- **14(C)** A verifying authority may digitally sign load modules or other executables with a digital signature that indicates or implies assurance level. A verifying authority can use digital signature techniques to distinguish between assurance levels. As one example, each different digital signature may be encrypted using a different verification key and/or fundamentally different encryption, one-way hash and/or other techniques. A protected processing environment or other secure execution space protects itself by

	Claim Term / Phrase	InterTrust Evidence
		executing only those load modules or other executables that have been digitally signed for its corresponding assurance level. '721 patent at 6:42-52. **14(D)** Figure 5 shows how a verifying authority can create a certifying digital signature Figure 6 shows how a protected processing environment can securely authenticate a verifying authority's digital signature to guarantee the integrity of the corresponding load module; Figure 7 shows how several different digital signatures can be applied to the same load module; Figure 8 shows how a load module can be distributed with multiple digital signatures '721 patent at 7:47-57. **14(E)** The two digital signature algorithms in widespread use today (RSA and DSA) are based on distinct mathematical problems (factoring in the case of RSA, discrete logs for DSA). '721 patent at 15:31-34. **14(F)** There exist many well known processes for creating digital signatures. One example is the Digital Signature Algorithm (DSA). DSA uses a public-key signature scheme that performs a pair of transformations to generate and verify a digital value called a "signature." '721 patent at 10:60-64.

	Claim Term / Phrase	InterTrust Evidence

Extrinsic Sources

14(G)

> **digital signature** In data security, a data block appended to a message, or a complete encrypted message, such that the recipient can authenticate the message contents and/or prove that it could only have originated with the purported sender. The digital signature is a function of: (a) the message, transaction or document to be signed; (b) secret information known only to the sender; and (c) public information employed in the validation process.
>
> Message authentication enables the receiver of a message to ensure that the contents cannot be changed accidentally or deliberately by a third party. However, since both the sender and the receiver share the same secret information there is no method of resolving disputes. The receiver can compute the authenticator and could therefore change a message, or forge a new message, develop the authenticator and claim that it was transmitted by the sender sharing the same secret key for authentication. Conversely the sender could disown an authenticated message and claim that the receiver produced a forged message using the common secret key.
>
> The essence of a digital signature is that the receiver must be able to prove that a message originated with a given sender, but must not be able to construct the signed message. Thus the sender requires secret information to construct the signed message and the receiver must be able to access public information for use in the validation of the message. In the case of a dispute the receiver must be in a position to supply non-secret information to a judge (i.e., the signed message and the publicly available information) in order to prove the authentication and origin of the message. *Compare* DYNAMIC PASSWORD. *See* MESSAGE AUTHENTICATION, PUBLIC KEY CRYPTOGRAPHY, RSA. *Synonymous with* ELECTRONIC SIGNATURE.

Dictionary of Information Technology, 3d ed. (Van Nostrand Reinhold, 1989), pp. 160-161.

Citations from Sources Designated by Microsoft under PLR 4-2(b)

14(H)

> **Digital signature** A string of characters that can be generated only by an agent that knows some secret, and hence provides evidence

	Claim Term / Phrase	InterTrust Evidence
		that such an agent must have generated it. Neumann, Computer Related Risks (ACM Press, 1995), p. 345. **14(I)** Another way to check your files for unauthorized tampering is to derive a signature for each file, and to compare that signature against a known value. A file signature is a function of the contents and properties of the file. A signature is relatively easy to calculate, but difficult to forge. Garfinkel et al., Practical Unix Security (O'Reilly & Associates, 1991), p. 122.

	Claim Term / Phrase	InterTrust Evidence
15.	**executable, executable programming** 721.34, 912.8, 912.35	<u>**Patent Specifications**</u> **15(A)** The next section of load module 1100 is an encrypted executable body 1106 that contains one or more blocks of encrypted code. Load modules 1100 are preferably coded in the "native" instruction set of their execution environment for efficiency and compactness. SPU 500 and platform providers may provide versions of the standard load modules 1100 in order to make their products cooperate with the content in distribution mechanisms contemplated by VDE 100. The preferred embodiment creates and uses native mode load modules 1100 in lieu of an interpreted or "p-code" solution to optimize the performance of a limited resource SPU. However, when sufficient SPE (or HPE) resources exist and/or platforms have sufficient resources, these other implementation approaches may improve the cross platform utility of load module code. '193 patent at 141:42-56. **15(B)** The load module or other executable is preferably constructed using a programming language (e.g., languages such as Java and Python) and/or design/implementation methodology (e.g., Gypsy, FDM) that can facilitate automated analysis, validation, verification, inspection, and/or testing. '721 patent at 5:34-39. <u>**Extrinsic Sources**</u> **15(C)** **executable** *adj.* Of, pertaining to, or being a program file that can be run. Executable files have extensions such as .bat, .com, and .exe. **executable** *n.* A program file that can be run, such as file0.bat, file1.exe, or file2.com. **executable program** *n.* A program that can be run. The term

	Claim Term / Phrase	InterTrust Evidence
		usually applies to a compiled program translated into machine code in a format that can be loaded into memory and run by a computer's processor. In interpreter languages, an executable program can be source code in the proper format. *See also* code (definition 1), compiler (definition 2), computer program, interpreter, source code. Microsoft Computer Dictionary, 3d ed. (Microsoft Press, 1997), p. 182.

	Claim Term / Phrase	InterTrust Evidence
16.	host processing environment 900.155	**Patent Specifications** **16(A)** Personal computer 4116 in this example is also provided with a secure processing unit 500 or software based HPE 655 (See Figure 12) to provide secure, tamper-resistant trusted processing. '683 patent at 20:16-19. **16(B)** "Protected Processing Environment" ("PPE") 650 may refer generally to SPE 503 and/or HPE 655. Hereinafter, unless context indicates otherwise, references to any of "PPE 650," "HPE 655" and "SPE 503" may refer to each of them. '193 patent at 105:18-22; '900 patent at 112:48-52. **16(C)** As discussed above in connection with Figure 12, each electronic appliance 600 in the preferred embodiment includes one or more SPEs 503 and/or one or more HPEs 655. These secure processing environments each provide a protected execution space for performing tasks in a secure manner. They may fulfill service requests passed to them by ROS 602, and they may themselves generate service requests to be satisfied by other services within ROS 602 or by services provided by another VDE electronic appliance 600 or computer. In the preferred embodiment, an SPE 503 is supported by the hardware resources of an SPU 500. An HPE 655 may be supported by general purpose processor resources and rely on software techniques for security/protection. HPE 655 thus gives ROS 602 the capability of assembling and executing certain component assemblies 690 on a general purpose CPU such as a microcomputer, minicomputer, mainframe computer or supercomputer processor. In the preferred embodiment, the overall software architecture of an SPE 503 may be the same as the software architecture of an HPE 655. An HPE 655 can "emulate" SPE 503 and associated SPU 500, i.e., each may include services and resources needed to support an identical set of service requests from ROS 602 (although ROS 602

	Claim Term / Phrase	InterTrust Evidence
		may be restricted from sending to an HPE certain highly secure tasks to be executed only within an SPU 500). '193 patent at 104:39-64; '900 patent at 112:2-27. **16(D)** In the preferred embodiment, HPE 655 is a secure processing environment supported by a processor other than an SPU, such as for example an electronic appliance CPU 654 general-purpose microprocessor or other processing system or device. In the preferred embodiment, HPE 655 may be considered to "emulate" an SPU 500 in the sense that it may use software to provide some or all of the processing resources provided in hardware and/or firmware by an SPU. HPE 655 in one preferred embodiment of the present invention is full-featured and fully compatible with SPE 503—that is, HPE 655 can handle each and every service call SPE 503 can handle such that the SPE and the HPE are "plug compatible" from an outside interface standpoint (with the exception that the HPE may not provide as much security as the SPE). '193 patent at 79:60-80:7; '900 patent at 87:32-46. **16(E)** Figure 12 also shows that ROS 602 may provide one or more SPEs 503 and/or one or more HPEs 655. As discussed above, HPE 655 may "emulate" an SPU 500 device, and such HPEs 655 may be integrated in lieu of (or in addition to) physical SPUs 500 for systems that need higher throughput. Some security may be lost since HPEs 655 are typically protected by operating system security and may not provide truly secure processing. Thus, in the preferred embodiment, for high security applications at least, all secure processing should take place within an SPE 503 having an execution space within a physical SPU 500 rather than a HPE 655 using software operating elsewhere in electronic appliance 600. '193 patent at 88:31-43; '900 patent at 96:6-18. **16(F)** Occurrence of the control operation demonstrates that

	Claim Term / Phrase	InterTrust Evidence
		microprocessor 2652 is executing in its most privileged "normal" mode and therefore can be trusted to execute successfully the "enter 'SPU' mode" sequence of instructions stored in secure memory 532. If microprocessor 2652 were not executing in its most privileged mode, there would be no assurance that those instructions would execute successfully. Because switch 2663 isolates microprocessor 2652 from external signals (e.g., interrupts) until "SPU" mode is successfully initialized, the entry instructions can be guaranteed to complete successfully. '900 patent at 78:30-40. **16(G)** Designing VDE capabilities into one or more standard microprocessor, microcontroller and/or other digital processing components may materially reduce VDE related hardware costs by employing the same hardware resources for both the transaction management uses contemplated by the present invention and for other, host electronic appliance functions. This means that a VDE SPU can employ (share) circuitry elements of a "standard" CPU. For example, if a "standard" processor can operate in protected mode and can execute VDE related instructions as a protected activity, then such an embodiment may provide sufficient hardware security for a variety of applications and the expense of a special purpose processor might be avoided. Under one preferred embodiment of the present invention, certain memory (e.g., RAM, ROM, NVRAM) is maintained during VDE related instruction processing in a protected mode (for example, as supported by protected mode microprocessors). '193 patent at 21:5-21; '900 patent at 21:1-17. **16(H)** A VDE node's hardware SPU is a core component of a VDE secure subsystem and may employ some or all of an electronic appliance's primary control logic, such as a microcontroller, microcomputer or other CPU arrangement. This primary control logic may be otherwise employed for non VDE purposes such as the control of some or all of an electronic appliance's non-VDE functions. When operating in a hardware SPU mode, said primary control logic must be sufficiently secure so as to protect and conceal important VDE

	Claim Term / Phrase	InterTrust Evidence
		processes. For example, a hardware SPU may employ a host electronic appliance microcomputer operating in protected mode while performing VDE related activities, thus allowing portions of VDE processes to execute with a certain degree of security. This alternate embodiment is in contrast to the preferred embodiment wherein a trusted environment is created using a combination of one or more tamper resistant semiconductors that are not part of said primary control logic. '193 patent at 49:33-50; '900 patent at 49:31-48.

	Claim Term / Phrase	InterTrust Evidence
17.	**identifier** 193.15, 912.8	**<u>Patent Specifications</u>** 17(A) This same termination (or other specified consequence such as budget reduction, price increase, message displays on screen to users, messages to administrators, etc.) can also be the consequence of the failure by a user or the users VDE installation to complete a monitored process, such as paying for usage in electronic currency, failure to perform backups of important stored information (e.g., content and/or appliance usage information, control information, etc.), failure to use a repeated failure to use the proper passwords or other identifiers, etc.). '193 patent at 270:12-21 17(B) During the same or different communication session, the terminal could similarly, securely communicate back to the portable appliance 2600 VDE secure subsystem details as to the retail transaction (for example, what was purchased and price, the retail establishment's digital signature, the retail terminal's identifier, tax related information, etc.). '193 patent at 233:35-41. 17(C) Many load modules 1100 contain code that executes in an SPE 503. Some load modules 1100 contain code that executes in an HPE 655. This allows methods 1000 to execute in whichever environment is appropriate. For example, an INFORMATION method 1000 can be built to execute only in SPE 503 secure space for government classes of security, or in an HPE 655 for commercial applications. As described above, the load module public header 802 may contain an "execution space code" field that indicates where the load module 1100 needs to execute. This functionality also allows for different SPE instruction sets as well as different user platforms, and allows methods to be constructed without dependencies on the underlying load module instruction set. '193 patent at 140:37-50.

	Claim Term / Phrase	InterTrust Evidence
		17(D) [VDE features] provide very flexible and extensible user identification according to individuals, installations, by groups such as classes, and by function and hierarchical identification employing a hierarchy of levels of client identification (for example, client organization ID, client department ID, client network ID, client project ID, and client employee ID, or any appropriate subset of the above). '193 patent at 25:31-38.
		17(E) Account Numbers and User IDs In the preferred embodiment, to control access to clearinghouses, users are assigned account numbers at clearinghouses. Account numbers provide a unique "instance" value for a secure database record from the point of view of an outsider. From the point of view of an electronic appliance 600 site, the user, group, or group/user ids provide the unique instance of a record. For example, from the point of view of VISA, your Gold Card belongs to account number #123456789. From the point of view of the electronic appliance site (for example, a server at a corporation), the Gold card might belong to user id 1023. In organizations which have plural users and/or user groups using a VDE node, such users and/or user groups will likely be assigned unique user IDs. '193 patent at 268:28-42.
		<u>**Extrinsic Sources**</u> **17(F)** **identify** v. **identified, identifying, identifies.** v. tr. **1.** To establish the identity of. **2.** To ascertain the origin, nature, or definitive characteristics of. **3.** *Biology*. To determine the taxonomic classification of (an organism). **4.** To consider as identical or united; equate. **5.** To associate or affiliate (oneself) closely with a person or group.v. intr. To establish an identification with another or others.[Medieval Latin *identificare*, to make to resemble : Late Latin *identitas*, identity. See IDENTITY + Latin *-ficare*, -fy.]--**i-den'ti-fi'a-ble** *adj*. --**i-den'ti-fi'a-bly** *adv*. --**i-den'ti-fi'er** *n*. American Heritage Dictionary, 3d ed. (Houghton Mifflin, 1992), p. 896.

	Claim Term / Phrase	InterTrust Evidence
18.	**protected processing environment** 683.2, 721.34	**Patent Specifications** **18(A)** Because security may be better/more effectively enforced with the assistance of hardware security features such as those provided by SPU 500 (and because of other factors such as increased performance provided by special purpose circuitry within SPU 500), at least one SPE 503 is preferred for many or most higher security applications. However, in applications where lesser security can be tolerated and/or the cost of an SPU 500 cannot be tolerated, the SPE 503 may be omitted and all secure processing may instead be performed by one or more secure HPEs 655 executing on general-purpose CPUs 654. '193 patent 80:65-81:8. **18(B)** The Ginter et al. patent disclosure describes, among other things, techniques for providing a secure, tamper resistant execution spaces within a "protected processing environment" for computer programs and data. The protected processing environment described in Ginter et al. may be hardware-based, software-based, or a hybrid. '721 patent 3:16-21. **18(C)** One particular example of a secure execution space is a "protected processing environment" 108 of the type shown in Ginter et al. (see Figures 6-12) and described in associated text. Protected processing environments 108 provide a secure execution environment in which appliances 58, 60, 62 may securely execute load modules 54 to perform useful tasks. '721 patent 8:33-40. **18(D)** In this example, appliance 600 may include one or more processors 4126 providing or supporting one or more "protected processing

	Claim Term / Phrase	InterTrust Evidence
		environments" (PPE) 650 (e.g., SPEs 503 and/or HPEs 544) shown in Figures 6-12 and 62-72). Protected processing environment 650 may, for example, be implemented using a secure processing unit (SPU) 500 of the type shown in Figure 9 and/or may be based on software tamper-resistance techniques or a combination of software and hardware. As described above in detail, protected processing environment 650 provides a secure, trusted environment for storing, manipulating, executing, modifying and otherwise processing secure information such as that provided in secure electronic containers 302. In this particular example, secure containers 302 may not be opened except within a protected processing environment 650. Protected processing environment 650 is provided with the cryptographic and other information it needs to open and manipulate secure containers 302, and is tamper resistant so that an attacker cannot easily obtain and use this necessary information. '683 patent 29:51-30:3.
		18(E) Figure 10 is a block diagram of one example of a software structure/architecture for Rights Operating System ("ROS") 602 provided by the preferred embodiment. In this example, ROS 602 includes an operating system ("OS") "core" 679, a user Application Program Interface ("API") 682, a "redirector" 684, an "intercept" 692, a User Notification/Exception Interface 686, and a file system 687. ROS 602 in this example also includes one or more Host Event Processing Environments ("HPEs") 655 and/or one or more Secure Event Processing Environments ("SPEs") 503 (these environments may be generically referred to as "Protected Processing Environments" 650). HPE(s) 655 and SPE(s) 503 are self-contained computing and processing environments that may include their own operating system kernel 688 including code and data processing resources. A given electronic appliance 600 may include any number of SPE(s) 503 and/or any number of HPE(s) 655. HPE(s) 655 and SPE(s) 503 may process information in a secure way, and provide secure processing support for ROS 602. For example, they may each perform secure processing based on one or more VDE component assemblies 690, and they may each offer secure processing services to OS kernel 680. In the preferred embodiment, SPE 503 is a secure processing environment provided at least in part by an SPU 500. Thus, SPU

	Claim Term / Phrase	InterTrust Evidence
		500 provides the hardware tamper-resistant barrier 503 surrounding SPE 503. SPE 503 provided by the preferred embodiment is preferably: small and compact loadable into resource constrained environments such as for example minimally configured SPUs 500 dynamically updatable extensible by authorized users integratable into object or procedural environments secure. In the preferred embodiment, HPE 655 is a secure processing environment supported by a processor other than an SPU, such as for example an electronic appliance CPU 654 general-purpose microprocessor or other processing system or device. In the preferred embodiment, HPE 655 may be considered to "emulate" an SPU 500 in the sense that it may use software to provide some or all of the processing resources provided in hardware and/or firmware by an SPU. HPE 655 in one preferred embodiment of the present invention is full-featured and fully compatible with SPE 503—that is, HPE 655 can handle each and every service call SPE 503 can handle such that the SPE and the HPE are "plug compatible" from an outside interface standpoint (with the exception that the HPE may not provide as much security as the SPE). HPEs 655 may be provided in two types: secure and not secure. For example, it may be desirable to provide non-secure versions of HPE 655 to allow electronic appliance 600 to efficiently run non-sensitive VDE tasks using the full resources of a fast general purpose processor or computer. Such non-secure versions of HPE 655 may run under supervision of an instance of ROS 602 that also includes an SPE 503. In this way, ROS 602 may run all secure processes within SPE 503, and only use HPE 655 for processes that do not require security but that may require (or run more efficiently) under potentially greater resources provided by a general purpose computer or processor supporting HPE 655. Non-secure and secure HPE 655 may operate together with a secure SPE 503. '193 patent 79:24-80:21.
		18(F) Figure 13 shows the software architecture of the preferred embodiment Secure Processing Environment (SPE) 503. This

	Claim Term / Phrase	InterTrust Evidence
		architecture may also apply to the preferred embodiment Host Processing Environment (HPE) 655. "Protected Processing Environment" ("PPE") 650 may refer generally to SPE 503 and/or HPE 655. '193 patent 105:15-20. **18(G)** In some embodiments and where commercially acceptable, certain VDE participants, such as clearinghouses that normally maintain sufficiently physically secure non-VDE processing environments, may be allowed to employ HPEs rather VDE hardware elements and interoperate, for example, with VDE end-users and content providers. '193 patent 13:17-23. **18(H)** An end user may make use of credit and/or currency securely stored within the end user's VDE installation secure subsystem to pay for charges related to use of VDE content received from the repository, and/or the user may maintain a secure credit and/or currency account remotely at the repository, including a "virtual" repository where payment is made for the receipt of such content by an end user. This later approach may provide greater assurance for payment to the repository and/or content providers particularly if the end user has only an HPE based secure subsystem. '193 patent 291:39-49. **18(I)** One way to inexpensively and conveniently deploy multiple instances of VDE electronic appliances 600 across a network would be to provide network workstations with software defining an HPE 655. This arrangement requires no hardware modification of the workstations; an HPE 655 can be defined using software only. An SPE(s) 503 and/or HPE(s) 655 could also be provided within a VDE server. This arrangement has the advantage of allowing distributed VDE network processing without requiring workstations to be

	Claim Term / Phrase	InterTrust Evidence
		customized or modified (except for loading a new program(s) into them). VDE functions requiring high levels of security may be restricted to an SPU-based VDE server. "Secure" HPE-based workstations could perform VDE functions requiring less security, and could also coordinate their activities with the VDE server. '193 patent 226:43-57. --- **18(J)** Large Organization Example In a somewhat more general example, suppose an organization (e.g., a corporation or government department) with thousands of employees and numerous offices disposed throughout a large geographic area wishes to exercise control over distribution of information which belongs to said organization (or association). '193 patent 277:26-32. --- **18(K)** User Environment In an organization (or association) such as that described above, users may utilize a variety of electronic appliances 600 for processing and managing documents. This may include personal computers, both networked and otherwise, powerful single-user workstations, and servers or mainframe computers. To provide support for the control information described in this example, each electronic appliance that participates in use and management of VDE-protected documents may be enhanced with a VDE secure subsystem supporting an SPE 503 and/or HPE 655. In some organizations, where the threats to secure operation are relatively low, an HPE 655 may suffice. In other organizations (e.g., government defense), it may be necessary to employ an SPE 503 in all situations where VDE-protected documents are processed. The choice of enhancement environment and technology may be different in different of the organization. Even if different types of PPE 650 are used within an organization to serve different

	Claim Term / Phrase	InterTrust Evidence
		requirements, they may be compatible and may operate on the same types (or subsets of types) of documents. '193 patent 278:45-65. **18(L)** This manufacturing process may include, [redacted], testing the bootstrap loader and challenge-response software permanently stored within PPE 650, and [redacted] '193 patent 223:36-39. **18(M)** [redacted]. '193 patent at 49:59-62. **18(N)** [redacted]. '193 patent at 221:2-6. **18(O)** VDE 100 provided by the preferred embodiment has [redacted]," and so that the time and cost to succeed in such a "brute force attack" substantially exceeds any value to be derived. In addition, the security provided by VDE 100 compartmentalizes the internal workings of VDE so that [redacted]

	Claim Term / Phrase	InterTrust Evidence
		bounded subset of protected information, not the entire system. '193 patent at 199:38-46. **18(P)** VDE supports trusted (sufficiently secure) electronic information distribution and usage control models for both commercial electronic content distribution and data security applications. '193 patent at 16:25-28. **18(Q)** 1. A security method comprising: (a) digitally signing a first load module with a first digital signature designating the first load module for use by a first device class; (b) digitally signing a second load module with a second digital signature different from the first digital signature, the second digital signature designating the second load module for use by a second device class having at least one of tamper resistance and security level different from the at least one of tamper resistance and security level of the first device class; (c) distributing the first load module for use by at least one device in the first device class; and (d) distributing the second load module for use by at least one device in the second device class. '721 patent at 21:9-24. **18(R)** 34. A protected processing environment comprising: a first tamper resistant barrier having a first security level, a first secure execution space, and

	Claim Term / Phrase	InterTrust Evidence
		at least one arrangement within the first tamper resistant barrier that prevents the first secure execution space from executing the same executable accessed by a second secure execution space having a second tamper resistant barrier with a second security level different from the first security level. '721 patent at 24:48-56. **18(S)** [VDE features] support security techniques that materially increase the time required to "break" a system's integrity. This includes using a collection of techniques that minimizes the damage resulting from comprising some aspect of the security features of the present inventions. '193 patent at 35:59-63. **18(T)** Fingerprinting electronic content before it is encrypted for transfer to a customer or other user provides information that can be very useful for identifying who received certain content which may have then been distributed or made available in unencrypted form. This information would be useful in tracking who may have "broken" the security of a VDE installation and was illegally making certain electronic content available to others. '193 patent at 38:4-12. **18(U)** If a content key becomes compromised, the portion of the content encrypted with the key is also compromised until the key "ages" and expires. If the "aging" process for that key also becomes compromised, then the breach becomes permanent. '193 patent at 222:49-53.

	Claim Term / Phrase	InterTrust Evidence
		18(V) If PPE 650 (or a VDE administrator watching its activities or communicating with it) detects that it has been compromised, it may be updated with an initialization to use new code, keys and new encryption/decryption algorithms. This would limit exposure to VDE objects 300 that existed at the time the encryption scheme was broken. '193 patent at 223:4-10. **18(W)** Secure VDE hardware (also known as SPUs for Secure Processing Units), or VDE installations that use software to substitute for, or complement, said hardware (provided by Host Processing Environments (HPEs)), operate in conjunction with secure communications, systems integration software, and distributed software control information and support structures, to achieve the electronic contract/rights protection environment of the present invention. '193 patent at 13:7-14. **<u>File Histories</u>** **18(X)** . . . the Examiner objects to the use of "environment" as indefinite and unclear. This word, however, is not used in isolation, but rather in the context of several longer phrases, all of which are defined in the specification. The phrase "protected processing environment," for example, is . . . described on at least, for example, pages 7-8 and 25 of the specification. . . . These terms are also described in the commonly assigned copending application . . . filed 13 February 1995. '721 Patent File History, 4/13/99 Amendment, p. 13.

	Claim Term / Phrase	InterTrust Evidence
		Citations from Sources Designated by Microsoft under PLR 4-2(b) **18(Y)** Furthermore, there is never an absolute sense in which a system is secure or reliable. Neumann, Computer Related Risks (ACM Press, 1995), p. 2. **18(Z)** The fundamental purpose of security is to minimize the risk of loss from (1) physical damage or destruction, (2) human errors and omissions, and (3) theft or unauthorized disclosure. That purpose is best fulfilled by effective loss-prevention efforts. Loss-prevention efforts involve the identification and assessment of risks to capital, human, informational, and technological assets, and the development of suitable and cost-feasible countermeasures. Hutt et al., Computer Security Handbook, 2d ed. (Macmillan, 1988), p. 75. **18(AA)** Total software security is no more attainable than is perfect security in any other area. A highly skilled programmer can almost always penetrate software safeguards written by another programmer. Of course, the same can be said for attorneys; an unprincipled lawyer can usually get around protections in a contract written by an-other lawyer. Yet contracts continue to be written, and, for the most part, they are effective. Computer software security routines can also be effective most of the time. A security procedure does not have to be all-encompassing, if it provides reasonable protection at an acceptable cost, it is certainly worthwhile. The basic consideration is one of degree—how important are specific elements of data and software, and how important is their security. Some data require very little security. For example, a software library containing programs that are similar to those found in many other computer installations does not require elaborate security protection against theft. On the other hand, proprietary programs and sensitive data require extensive

	Claim Term / Phrase	InterTrust Evidence
		security. A data base containing payroll information requires stringent security procedures to maintain its confidentiality. Hutt et al., Computer Security Handbook, 2d ed. (Macmillan, 1988), p. 201. **18(BB)** Regardless of which form of data storage is being considered, one must bear in mind a vital concept, no data processing installation can afford 100 percent security—if indeed there is such a thing. Hutt et al., Computer Security Handbook, 2d ed. (Macmillan, 1988), p. 218. **18(CC)** One hundred percent security cannot be achieved. The most effective systems apply security protection techniques in layers. Each layer of protection diminishes the chances of someone breaking through the barriers. Hutt et al., Computer Security Handbook, 2d ed. (Macmillan, 1988), pp. 293. **18(DD)** Risk analysis is not intended to come up with a plan for absolute security. Indeed, absolute security is not achievable in today's computer's systems. Rather, risk analysis produces a degree of security commensurate with the information to be protected and with the amount of resources to be expended. Hoffman, Modern Methods for Computer Security and Privacy (Prentice-Hall, 1977), p. 170. **18(EE)** No matter how secure you make them, computers can always be broken into given sufficient resources, time, and money. Computers are especially vulnerable because software is complex and we don't always know if there are flaws present that make the task of breaking in easier. Even systems that are certified according to the

	Claim Term / Phrase	InterTrust Evidence
		Department of Defense's so-called Orange Book are vulnerable, especially if they are not administered correctly. Just as six-foot-thick vaults doors don't work if they're not administered properly. Garfinkel et al., Practical Unix Security (O'Reilly & Associates, 1991), pp. 13. **18(FF)** Security is a relative, not an absolute, concept, and gains in security often come only with penalties in performance. Landwehr, Formal Models for Computer Security, ACM Computer Surveys (Sept. 3, 1981), p. 253.

	Claim Term / Phrase	InterTrust Evidence
19.	secure, securely 193.1, 193.11, 193.15, 861.58, 891.1, 683.2, 721.34, 912.8, 912.35	**Patent Specifications** **19(A)** VDE normally employs an integration of cryptographic and other security technologies (e.g. encryption, digital signatures, etc.), with other technologies . . . . '193 patent 8:1-3. **19(B)** Since VDE also employs secure (e.g. encrypted and authenticated) communications when passing information between the participant location (nodes) secure subsystems of a VDE arrangement, important components of a VDE electronic agreement can be reliably enforced with sufficient security (sufficiently trusted) for the intended commercial purposes. '193 patent 45:39-45. **19(C)** The degree of overall security of the VDE system is primarily dependent on the degree of tamper resistance and concealment of VDE control process execution and related data storage activities. '193 patent 21:26-29. **19(D)** Because of the VDE security, including use of effective encryption, authentication, digital signaturing, and secure database structures, the records contained within a VDE card arrangement may be accepted as valid transaction records for government and/or corporate recordkeeping requirements. '193 patent 41:37-42.

	Claim Term / Phrase	InterTrust Evidence
		19(E) SPU 500 is enclosed within and protected by a "tamper resistant security barrier" 502. Security barrier 502 separates the secure environment 503 from the rest of the world. It prevents information and processes within the secure environment 503 from being observed, interfered with and leaving except under appropriate secure conditions. Barrier 502 also controls external access to secure resources, processes and information within SPU 500. In one example, tamper resistant security barrier 502 is formed by security features such as "encryption," and hardware that detects tampering and/or destroys sensitive information within secure environment 503 when tampering is detected. '193 patent 59:48-59.
		19(F) VDE 100 stores separately deliverable VDE elements in a secure (e.g., encrypted) database 610 distributed to each VDE electronic appliance 610. '193 patent 126:6-8.
		19(G) Secure (tamper-resistant) executable code. '193 patent 126:30-31.
		19(H) In one embodiment, the portable appliance 2600 could support secure (in this instance encrypted and/or authenticated) two-way communications with a retail terminal which may contain a VDE electronic appliance 600 or communicate with a retailer's or third party provider's VDE electronic appliance 600. '193 patent 233:25-30.

	Claim Term / Phrase	InterTrust Evidence
		19(I) Information could then be automatically "parsed" and routed into securely maintained (for example, encrypted) appropriate database management records within portable appliance 2600. '193 patent 233:51-54.
		19(J) The level of security and tamper resistance required for trusted SPU hardware processes depends on the commercial requirements of particular markets or market niches, and may vary widely. '193 patent at 49:59-62.
		19(K) There are many ways in which a PPE 650 might be compromised. The goal of the security provided by VDE 100 is to reduce the possibility that the system will be compromised, and minimize the adverse effects if it is compromised. '193 patent at 221:2-6.
		19(L) VDE 100 provided by the preferred embodiment has sufficient security to help ensure that it cannot be compromised short of a successful "brute force attack," and so that the time and cost to succeed in such a "brute force attack" substantially exceeds any value to be derived. In addition, the security provided by VDE 100 compartmentalizes the internal workings of VDE so that a successful "brute force attack" would compromise only a strictly bounded subset of protected information, not the entire system. '193 patent at 199:38-46.
		19(M) VDE supports trusted (sufficiently secure) electronic information

	Claim Term / Phrase	InterTrust Evidence
		distribution and usage control models for both commercial electronic content distribution and data security applications. '193 patent at 16:25-28.
		19(N) Because security may be better/more effectively enforced with the assistance of hardware security features such as those provided by SPU 500 (and because of other factors such as increased performance provided by special purpose circuitry within SPU 500), at least one SPE 503 is preferred for many or most higher security applications. However, in applications where lesser security can be tolerated and/or the cost of an SPU 500 cannot be tolerated, the SPE 503 may be omitted and all secure processing may instead be performed by one or more secure HPEs 655 executing on general-purpose CPUs 654. '193 patent at 80:65-81:8.
		19(O) 1. A security method comprising: (a) digitally signing a first load module with a first digital signature designating the first load module for use by a first device class; (b) digitally signing a second load module with a second digital signature different from the first digital signature, the second digital signature designating the second load module for use by a second device class having at least one of tamper resistance and security level different from the at least one of tamper resistance and security level of the first device class; (c) distributing the first load module for use by at least one device in the first device class; and (d) distributing the second load module for use by at least one device in the second device class. '721 patent at 21:9-24.

	Claim Term / Phrase	InterTrust Evidence
		19(P) 34. A protected processing environment comprising: a first tamper resistant barrier having a first security level, a first secure execution space, and at least one arrangement within the first tamper resistant barrier that prevents the first secure execution space from executing the same executable accessed by a second secure execution space having a second tamper resistant barrier with a second security level different from the first security level. '721 patent at 24:48-56. **19(Q)** [VDE features] support security techniques that materially increase the time required to "break" a system's integrity. This includes using a collection of techniques that minimizes the damage resulting from comprising some aspect of the security features of the present inventions. '193 patent at 35:59-63. **19(R)** Fingerprinting electronic content before it is encrypted for transfer to a customer or other user provides information that can be very useful for identifying who received certain content which may have then been distributed or made available in unencrypted form. This information would be useful in tracking who may have "broken" the security of a VDE installation and was illegally making certain electronic content available to others. '193 patent at 38:4-12. **19(S)** If a content key becomes compromised, the portion of the content encrypted with the key is also compromised until the key "ages" and

	Claim Term / Phrase	InterTrust Evidence
		expires. If the "aging" process for that key also becomes compromised, then the breach becomes permanent. '193 patent at 222:49-53. **19(T)** If PPE 650 (or a VDE administrator watching its activities or communicating with it) detects that it has been compromised, it may be updated with an initialization to use new code, keys and new encryption/decryption algorithms. This would limit exposure to VDE objects 300 that existed at the time the encryption scheme was broken. '193 patent at 223:4-10. **<u>Extrinsic Sources</u>** **19(U)** **security** The protection of valuable assets stored on computer systems or transmitted via computer networks. Computer security involves the following conceptually differentiated areas: • **Authentication** (ensuring that users are indeed the persons they claim to be). • **Access control** (ensuring that users access only those resources and services that they are entitled to access). • **Confidentiality** (ensuring that transmitted or stored data is not examined by unauthorized persons). • **Integrity** (ensuring that transmitted or stored data is not altered by unauthorized persons in a way that is not detectable by authorized users). • **Nonrepudiation** (ensuring that qualified users are not denied access to services that they legitimately expect to receive, and that originators of messages cannot deny that they in fact sent a given message). Webster's New World Dictionary of Computer Terms, 6th ed. (1997), p. 463.

	Claim Term / Phrase	InterTrust Evidence
		<u>Citations from Sources Designated by Microsoft under PLR 4-2(b)</u> **19(V)** In common technical usage, however, computer security and communication security generally refer to protection against human misuse, and exclude the protection against malfunctions. Neumann, Computer Related Risks (ACM Press, 1995), p. 96. **19(W)** There is a fifth important attribute of dependability—the *security attribute*—that cannot be measured easily: the ability of a system to prevent unauthorized access or handling of information. Mullender, Distributed Systems, 2nd ed. (Addison-Wesley, 1993), p. 420. **19(X)** Furthermore, there is never an absolute sense in which a system is secure or reliable. Neumann, Computer Related Risks (ACM Press, 1995), p. 2. **19(Y)** The fundamental purpose of security is to minimize the risk of loss from (1) physical damage or destruction, (2) human errors and omissions, and (3) theft or unauthorized disclosure. That purpose is best fulfilled by effective loss-prevention efforts. Loss-prevention efforts involve the identification and assessment of risks to capital, human, informational, and technological assets, and the development of suitable and cost-feasible countermeasures. Hutt et al., Computer Security Handbook, 2d ed. (Macmillan, 1988), p. 75. **19(Z)** Total software security is no more attainable than is perfect security in any other area. A highly skilled programmer can almost

	Claim Term / Phrase	InterTrust Evidence
		always penetrate software safeguards written by another programmer. Of course, the same can be said for attorneys; an unprincipled lawyer can usually get around protections in a contract written by an-other lawyer. Yet contracts continue to be written, and, for the most part, they are effective. Computer software security routines can also be effective most of the time. A security procedure does not have to be all-encompassing, if it provides reasonable protection at an acceptable cost, it is certainly worthwhile. The basic consideration is one of degree—how important are specific elements of data and software, and how important is their security. Some data require very little security. For example, a software library containing programs that are similar to those found in many other computer installations does not require elaborate security protection against theft. On the other hand, proprietary programs and sensitive data require extensive security. A data base containing payroll information requires stringent security procedures to maintain its confidentiality. Hutt et al., Computer Security Handbook, 2d ed. (Macmillan, 1988), p. 201.
		19(AA) Regardless of which form of data storage is being considered, one must bear in mind a vital concept: no data processing installation can afford 100 percent security—if indeed there is such a thing. Hutt et al., Computer Security Handbook, 2d ed. (Macmillan, 1988), p. 218.
		19(BB) One hundred percent security cannot be achieved. The most effective systems apply security protection techniques in layers. Each layer of protection diminishes the chances of someone breaking through the barriers. Hutt et al., Computer Security Handbook, 2d ed. (Macmillan, 1988), pp. 293.
		19(CC) Risk analysis is not intended to come up with a plan for absolute security. Indeed, absolute security is not achievable in today's

	Claim Term / Phrase	InterTrust Evidence
		computer's systems. Rather, risk analysis produces a degree of security commensurate with the information to be protected and with the amount of resources to be expended. Hoffman, Modern Methods for Computer Security and Privacy (Prentice-Hall, 1977), p. 170. **19(DD)** No matter how secure you make them, computers can always be broken into given sufficient resources, time, and money. Computers are especially vulnerable because software is complex and we don't always know if there are flaws present that make the task of breaking in easier. Even systems that are certified according to the Department of Defense's so-called Orange Book are vulnerable, especially if they are not administered correctly. Just as six-foot-thick vaults doors don't work if they're not administered properly. Garfinkel et al., Practical Unix Security (O'Reilly & Associates, 1991), pp. 13. **19(EE)** Security is a relative, not an absolute, concept, and gains in security often come only with penalties in performance. Landwehr, Formal Models for Computer Security, ACM Computer Surveys (Sept. 3, 1981), p. 253.

	Claim Term / Phrase	InterTrust Evidence
20.	**secure container** 912.35, 861.58, 683.2	**Patent Specifications** **20(A)** The "container" concept is a convenient metaphor used to give a name to the collection of elements required to make use of content or to perform an administrative-type activity. Container 302 typically includes identifying information, control structures and content (e.g., a property or administrative data). The term "container" is often (e.g., Bento/OpenDoc and OLE) used to describe a collection of information stored on a computer system's secondary storage system(s) or accessible to a computer system over a communications network on a "server's" secondary storage system. The "container" 302 provided by the preferred embodiment is not so limited or restricted. In VDE 100, there is no requirement that this information is stored together, received at the same time, updated at the same time, used for only a single object, or be owned by the same entity. Rather, in VDE 100 the container concept is extended and generalized to include real-time content and/or online interactive content passed to an electronic appliance over a cable, by broadcast, or communicated by other electronic communication means. '193 patent 127:30-49. **20(B)** VDE, in its preferred embodiment, employs object software technology and uses object technology to form "containers" for delivery of information that is (at least in part) encrypted or otherwise secured. These containers may contain electronic content products or other electronic information and some or all of their associated permissions (control) information. These container objects may be distributed along pathways involving content providers and/or content users. They may be securely moved among nodes of a Virtual Distribution Environment (VDE) arrangement, which nodes operate VDE foundation software and execute control methods to enact electronic information usage control and/or administration models. The containers delivered through use of the preferred embodiment of the present invention may be employed both for distributing VDE control instructions (information) and/or to encapsulate and electronically distribute content that has been at least partially secured. '193 patent 13:54-14:4.

	Claim Term / Phrase	InterTrust Evidence
		20(C) Figure 88 illustrates secure electronic container 302 as an attaché case handcuffed to the secure delivery person's wrist. Once again, container is shown as a physical thing for purposes of illustration only -- in the example it is preferably electronic rather than physical, and comprises digital information having a well-defined structure (see Figure 5A). Special mathematical techniques known as "cryptography" can be used to make electronic container 302 secure so that only intended recipient 4056 can open the container and access the electronic document (or other item) 4054 it contains. '683 patent 15:61-16:4.
		20(D) The Figure 5A example shows items "within" and enclosed by container 302. However, container 302 may "contain" items without those items actually being stored within the container. For example, the container 302 may reference items that are available elsewhere such as in other containers at remote sites. Container 302 may reference items available at different times or only during limited times. Some items may be too large to store within container 302. Items may, for example, be delivered to the user in the form of a "live feed" of video at a certain time. Even then, the container 302 "contains" the live feed (by reference) in this example. '193 patent 58:48-58.
		20(E) The term "container" is often (e.g., Bento/OpenDoc and OLE) used to describe a collection of information stored on a computer system's secondary storage system(s) or accessible to a computer system over a communications network on a "server's" secondary storage system. The "container" 302 provided by the preferred embodiment is not so limited or restricted. In VDE 100, there is no requirement that this information is stored together, received at the same time, updated at the same time, used for only a single object, or be owned by the same entity. Rather, in VDE 100 the container concept is extended and generalized to include real-time content and/or online interactive content passed to an electronic appliance

	Claim Term / Phrase	InterTrust Evidence
		over a cable, by broadcast, or communicated by other electronic communication means. Thus, the "complete" VDE container 302 or logical object structure 800 may not exist at the user's location (or any other location, for that matter) at any one time. The "logical object" may exist over a particular period of time (or periods of time), rather than all at once. This concept includes the notion of a "virtual container" where important container elements may exist either as a plurality of locations and/or over a sequence of time periods (which may or may not overlap). Of course, VDE 100 containers can also be stored with all required control structures and content together. This represents a continuum: from all content and control structures present in a single container, to no locally accessible content or container specific control structures. '193 patent 127:35-62.
		20(F) In order to improve performance, the containers themselves may remain at the users' sites, and only the encrypted contents transmitted between the participants. '683 patent 53:3-5.
		20(G) In more detail, the logical object structure 800 provided by the preferred embodiment includes a public (or unencrypted) header 802 that identifies the object and may also identify one or more owners of rights in the object and/or one or more distributors of the object. Private (or encrypted) header 804 may include a part or all of the information in the public header and further, in the preferred embodiment, will include additional data for validating and identifying the object 300 when a user attempts to register as a user of the object with a service clearinghouse, VDE administrator, or an SPU 500. Alternatively, information identifying.... '193 patent 128:11-21.

	Claim Term / Phrase	InterTrust Evidence
		20(H) Third party go-between can authenticate an item by, for example, opening (e.g. decrypting content) one or more containers '683 patent 9:59-61. --- **Extrinsic Sources** **20(I)** **container** *n.* **1.** In OLE terminology, a file containing linked or embedded objects. *See also* OLE. **2.** In SGML, an element that has content as opposed to one consisting solely of the tag name and attributes. Microsoft Computer Dictionary, 3d, ed. (Microsoft Press, 1997), p. 115. --- **20(J)** In a preferred embodiment of the present invention, an application program that creates a compound document controls the manipulation of linked or embedded data generated by another application. In object-oriented parlance, this data is referred to as an object. (The reference Budd, T., "An Introduction to Object-Oriented Programming," Addison-Wesley Publishing Co., Inc., 1991, provides an introduction to object-oriented concepts and terminology.) An object that is either linked or embedded into a compound document is "contained" within the document. Also, a compound document is referred to as a "container" object and the objects contained within a compound document are referred to as "contained" or "containee" objects. Referring to FIGS. 1 and 2, the scheduling data 102 and budgeting data 103 are containee objects and the compound document 101 is a container object. USP 5,634,019 at 7:34-49.

	Claim Term / Phrase	InterTrust Evidence
21.	**tamper resistance** 721.1	**<u>Patent Specifications</u>** **21(A)** Maintaining shared secrets (e.g., cryptographic keys) within a tamper resistant enclosure that the owner of the electronic appliance cannot easily tamper with. '721 patent at 4:40-42. **21(B)** SPU 500 is enclosed within and protected by a "tamper resistant security barrier" 502. Security barrier 502 separates the secure environment 503 from the rest of the world. It prevents information and processes within the secure environment 503 from being observed, interfered with and leaving except under appropriate secure conditions. Barrier 502 also controls external access to secure resources, processes and information within SPU 500. In one example, tamper resistant security barrier 502 is formed by security features such as "encryption," and hardware that detects tampering and/or destroys sensitive information within secure environment 503 when tampering is detected. '193 patent at 59:48-59. **<u>Extrinsic Sources</u>** **21(C)** To evaluate the results of physically protecting portions of the system, the concept of a tamper-resistant module (TRM) is introduced. All information contained within a TRM is protected from disclosure and undetected modification in the following sense. As long as the TRM is intact, data inside the module cannot be discerned or modified by an attacker and if the TRM is breached the sensitive data within is destroyed (erased). The implementation of TRMs will vary considerably depending on the value of the external software being protected and the perceived sophistication of potential attackers. Kent, Protecting Externally Supplied Software in Small Computers, Doctoral Thesis (Sept. 22, 1980), p. PA00000363.

	Claim Term / Phrase	InterTrust Evidence
		21(D) Tamper resistant software is software which is resistant to observation and modification. It can be trusted/ within certain bounds/ to operate as intended even in the presence of a malicious attack. Our approach has been to classify attacks into three categories and then to develop a series of software design principles that allow a scaled response to those threats. Aucsmith, Tamper Resistant Software: An Implementation (1996), p. PA00002323. **21(E)** Tamper-resistance ensures proper operation of a program and prevents extraction of secret data and abuse of the program. Moreover tamper-resistance enables a vendor to enforce his own conditions upon users. Mambo et al., A Tentative Approach to Constructing Tamper-Resistant Software, School of Information Science, Japan Advanced Institute of Science and Technology, 1-1 Asahidai Tatsunokuchi Nomi, Ishikawa (1997), p. PA00005363.

	Claim Term / Phrase	InterTrust Evidence
22.	tamper resistant barrier 721.34	**<u>Patent Specifications</u>** **22(A)** SPU 500 is enclosed within and protected by a "tamper resistant security barrier" 502. Security barrier 502 separates the secure environment 503 from the rest of the world. It prevents information and processes within the secure environment 503 from being observed, interfered with and leaving except under appropriate secure conditions. Barrier 502 also controls external access to secure resources, processes and information within SPU 500. In one example, tamper resistant security barrier 502 is formed by security features such as "encryption," and hardware that detects tampering and/or destroys sensitive information within secure environment 503 when tampering is detected. '193 patent 59:48-59. **22(B)** HPEs 655 may (as shown in Figure 10) be provided with a software-based tamper resistant barrier 674 that makes them more secure. Such a software-based tamper resistant barrier 674 may be created by software executing on general-purpose CPU 654. Such a "secure" HPE 655 can be used by ROS 602 to execute processes that, while still needing security, may not require the degree of security provided by SPU 500. This can be especially beneficial in architectures providing both an SPE 503 and an HPE 655. The SPU 502 may be used to perform all truly secure processing, whereas one or more HPEs 655 may be used to provide additional secure (albeit possibly less secure than the SPE) processing using host processor or other general purpose resources that may be available within an electronic appliance 600. Any service may be provided by such a secure HPE 655. In the preferred embodiment, certain aspects of "channel processing" appears to be a candidate that could be readily exported from SPE 503 to HPE 655. The software-based tamper resistant barrier 674 provided by HPE 655 may be provided, for example, by: introducing time checks and/or code modifications to complicate the process of stepping through code comprising a portion of kernel 688a and/or a portion of component assemblies 690 using a debugger; using a map of defects on a storage device (e.g., a hard disk, memory card, etc.) to form internal test values to impede moving and/or copying HPE 655 to other electronic appliances 600; using kernel code that contains

	Claim Term / Phrase	InterTrust Evidence
		false branches and other complications in flow of control to disguise internal processes to some degree from disassembly or other efforts to discover details of processes; using "self-generating" code (based on the output of a co-sine transform, for example) such that detailed and/or complete instruction sequences are not stored explicitly on storage devices and/or in active memory but rather are generated as needed; using code that "shuffles" memory locations used for data values based on operational parameters to complicate efforts to manipulate such values; using any software and/or hardware memory management resources of electronic appliance 600 to "protect" the operation of HPE 655 from other processes, functions, etc. Although such a software-based tamper resistant barrier 674 may provide a fair degree of security, it typically will not be as secure as the hardware-based tamper resistant barrier 502 provided (at least in part) by SPU 500. '193 patent 80:22-65. **22(C)** Protected execution spaces such as protected processing environments can be programmed or otherwise conditioned to accept only those load modules or other executables bearing a digital signature/certificate of an accredited (or particular) verifying authority. Tamper resistant barriers may be used to protect this programming or other conditioning. '721 patent 5:1-6.

	Claim Term / Phrase	InterTrust Evidence
23.	**use** 912.8, 912.35, 861.58, 193.19, 891.1, 683.2, 721.1	**<u>Extrinsic Sources</u>** **23(A)** **use** *v.* **used, us-ing, us-es.** *tr.* **1.** To put into service or apply for a purpose; employ. **2.** To avail oneself of; practice: *use caution.* **3.** To conduct oneself toward; treat or handle: *"the peace offering of a man who once used you unkindly"* (Laurence Sterne). **4.** To seek or achieve an end by means of; exploit: *used their highly placed friends to gain access to the president; felt he was being used by seekers of favor.* **5.** To take or consume; partake of: *She rarely used alcohol.* –intr. (yoos, yoost). Used in the past tense followed by *to* in order to indicate a former state, habitual practice, or custom: *Mail service used to be faster.* **use** (yoos). *n.* **1. a.** The act of using; the application or employment of something for a purpose: *with the use of a calculator; skilled in the use of the bow and arrow.* **b.** The condition or fact of being used: *a chair in regular use.* **2.** The manner of using; usage: *learned the proper use of power tools.* **3. a.** The permission, privilege, or benefit of using something: *gave us the use of their summerhouse.* **b.** The power or ability to use something: *lost the use of one arm.* **4.** The need or occasion to use or employ: *have no use for these old clothes.* **5.** The quality of being suitable or adaptable to an end; usefulness: *tried to be of use in the kitchen.* **6.** A purpose for which something is used: *a tool with several uses; a pretty bowl, but of what use is it?* **7.** Gain or advantage; good: *There's no use in discussing it. What's the use?* **8.** Accustomed or usual procedure or practice. **9.** *Law.* **a.** Enjoyment of property, as by occupying or exercising it. **b.** The benefit or profit of lands and tenements of which the legal title and possession are vested in another. **c.** The arrangement establishing the equitable right to such benefits and profits. **10.** A liturgical form practiced in a particular church, ecclesiastical district, or community. **11.** *Obsolete*. Usual occurrence or experience. **--phrasal verb. use up.** To consume completely: *used up all our money.* [Middle English *usen*, from Old French *user*, from Vulgar Latin **usare*, frequentative of Latin *uti.*] *SYNONYM: use, employ, utilize.* These verbs mean to avail oneself of someone or something in order to make him, her, or it useful, functional, or beneficial. To *use* is to put into service or apply for a purpose: *uses a hearing aid; used the press secretary as spokesperson for the administration; using a stick to stir the paint. Employ* is often interchangeable with *use*: *She employed her education to maximum advantage.* Unlike *use*, however, the term can denote engaging or maintaining the services of another or putting another to work: *"When men are employed, they are best*

	Claim Term / Phrase	InterTrust Evidence
		contented" (Benjamin Franklin). *Utilize* is especially appropriate in the narrower sense of making something profitable or of finding new and practical uses for it: *In the 19th century waterpower was widely utilized to generate electricity.* See also Synonyms at **habit.** American Heritage Dictionary, 3d ed. (Houghton Mifflin, 1992), p. 1966.

	Claim Term / Phrase	InterTrust Evidence
24.	**virtual distribution environment** 900.155	**<u>Patent Specifications</u>** **24(A)** VDE provides a secure, distributed electronic transaction management system for controlling the distribution and/or other usage of electronically provided and/or stored information. '193 patent at 9:36-39; '900 patent at 9:33-36. **24(B)** Electronic appliances such as computers employed in accordance with the present invention help to ensure that information is accessed and used only in authorized ways, and maintain the integrity, availability, and/or confidentiality of the information. Secure subsystems used with such electronic appliances provide a distributed virtual distribution environment (VDE) that may enforce a secure chain of handling and control, for example, to control and/or meter or otherwise monitor use of electronically stored or disseminated information. Such a virtual distribution environment may be used to protect rights of various participants in electronic commerce and other electronic or electronic-facilitated transactions. '900 patent at Abstract. **24(C)** Figure 1 shows a "Virtual Distribution Environment" ("VDE") 100 that may be provided in accordance with this invention. In Figure 1, an information utility 200 connects to communications means 202 such as telephone or cable TV lines for example. Telephone or cable TV lines 202 may be part of an "electronic highway" that carries electronic information from place to place. Lines 202 connect information utility 200 to other people such as for example a consumer 208, an office 210, a video production studio 204, and a publishing house 214. Each of the people connected to information utility 200 may be called a "VDE participant" because they can participate in transactions occurring within the virtual distribution environment 100. Almost any sort of transaction you can think of can be supported by virtual distribution environment 100. A few of many examples of

	Claim Term / Phrase	InterTrust Evidence
		transactions that can be supported by virtual distribution environment 100 include: home banking and electronic payments; electronic legal contracts; distribution of "content" such as electronic printed matter, video, audio, images and computer programs; and secure communication of private information such as medical records and financial information. Virtual distribution environment 100 is "virtual" because it does not require many of the physical "things" that used to be necessary to protect rights, ensure reliable and predictable distribution, and ensure proper compensation to content creators and distributors. For example, in the past, information was distributed on records or disks that were difficult to copy. In the past, private or secret content was distributed in sealed envelopes or locked briefcases delivered by courier. To ensure appropriate compensation, consumers received goods and services only after they handed cash over to a seller. Although information utility 200 may deliver information by transferring physical "things" such as electronic storage media, the virtual distribution environment 100 facilitates a completely electronic "chain of handling and control." '193 patent at 52:66-53:37; '900 patent 53:39-54:10. **24(D)** Because security may be better/more effectively enforced with the assistance of hardware security features such as those provided by SPU 500 (and because of other factors such as increased performance provided by special purpose circuitry within SPU 500), at least one SPE 503 is preferred for many or most higher security applications. However, in applications where lesser security can be tolerated and/or the cost of an SPU 500 cannot be tolerated, the SPE 503 may be omitted and all secure processing may instead be performed by one or more secure HPEs 655 executing on general-purpose CPUs 654. '193 patent 80:65-67-81:8.

	Claim Term / Phrase	InterTrust Evidence
		24(E) An end user may make use of credit and/or currency securely stored within the end user's VDE installation secure subsystem to pay for charges related to use of VDE content received from the repository, and/or the user may maintain a secure credit and/or currency account remotely at the repository, including a "virtual" repository where payment is made for the receipt of such content by an end user. This later approach may provide greater assurance for payment to the repository and/or content providers particularly if the end user has only an HPE-based secure subsystem. '193 patent at 291:39-49; '900 patent 316:35-45. **24(F)** Large Organization Example In a somewhat more general example, suppose an organization (e.g., a corporation or government department) with thousands of employees and numerous offices disposed throughout a large geographic area wishes to exercise control over distribution of information which belongs to said organization (or association). '193 patent at 277:26-32; '900 patent 302:17-24. **24(G)** User Environment In an organization (or association) such as that described above, users may utilize a variety of electronic appliances 600 for processing and managing documents. This may include personal computers, both networked and otherwise, powerful single-user workstations, and servers or mainframe computers. To provide support for the control information described in this example, each electronic appliance that participates in use and management of VDE-protected documents may be enhanced with a VDE secure subsystem supporting an SPE 503 and/or HPE 655. In some organizations, where the threats to secure operation are relatively low, an HPE 655 may suffice. In other organizations (e.g., government defense), it may be necessary to employ an SPE

	Claim Term / Phrase	InterTrust Evidence
		503 in all situations where VDE-protected documents are processed. The choice of enhancement environment and technology may be different in different of the organization. Even if different types of PPE 650 are used within an organization to serve different requirements, they may be compatible and may operate on the same types (or subsets of types) of documents. '193 patent at 278:45-65; '900 patent 303:40-61. **24(H)** HPEs 655 may (as shown in Figure 10) be provided with a software-based tamper resistant barrier 674 that makes them more secure. Such a software-based tamper resistant barrier 674 may be created by software executing on general-purpose CPU 654. Such a "secure" HPE 655 can be used by ROS 602 to execute processes that, while still needing security, may not require the degree of security provided by SPU 500. This can be especially beneficial in architectures providing both an SPE 503 and an HPE 655. The SPU 502 may be used to perform all truly secure processing, whereas one or more HPEs 655 may be used to provide additional secure (albeit possibly less secure than the SPE) processing using host processor or other general purpose resources that may be available within an electronic appliance 600. Any service may be provided by such a secure HPE 655. In the preferred embodiment, certain aspects of "channel processing" appears to be a candidate that could be readily exported from SPE 503 to HPE 655. The software-based tamper resistant barrier 674 provided by HPE 655 may be provided, for example, by: introducing time checks and/or code modifications to complicate the process of stepping through code comprising a portion of kernel 688a and/or a portion of component assemblies 690 using a debugger; using a map of defects on a storage device (e.g., a hard disk, memory card, etc.) to form internal test values to impede moving and/or copying HPE 655 to other electronic appliances 600; using kernel code that contains false branches and other complications in flow of control to disguise internal processes to some degree from disassembly or other efforts to discover details of processes; using "self-generating" code (based on the output of a co-sine transform, for example) such that detailed and/or complete instruction sequences are not stored explicitly on storage devices and/or in active memory but rather are generated as needed; using code that "shuffles" memory locations used for data values based on operational parameters to complicate efforts to manipulate such values; using any software and/or hardware

	Claim Term / Phrase	InterTrust Evidence
		memory management resources of electronic appliance 600 to "protect" the operation of HPE 655 from other processes, functions, etc. Although such a software-based tamper resistant barrier 674 may provide a fair degree of security, it typically will not be as secure as the hardware-based tamper resistant barrier 502 provided (at least in part) by SPU 500. '193 patent 80:22-65. **24(I)** VDE supplies an efficient, largely transparent, low cost and sufficiently secure system (supporting both hardware/software and software only models). '193 patent at 9:11-13; '900 patent 9:8-10. **24(J)** 10. A method as in claim 1 in which said steps of receiving, providing, performing and producing occur within a Virtual Distribution Environment. 11. A system as in claim 2 in which said first location and said second location are contained within a Virtual Distribution Environment. 12. A system as in claim 3 in which said first location and said second location are contained within a Virtual Distribution Environment. 13. A system as in claim 6 in which said protected processing environment is contained within a Virtual Distribution Environment. 14. A method as in claim 9 in which said first location and said second location are contained within a Virtual Distribution Environment. USP 5,949,876 at 320:14-28.

	Claim Term / Phrase	InterTrust Evidence
		24(K) The level of security and tamper resistance required for trusted SPU hardware processes depends on the commercial requirements of particular markets or market niches, and may vary widely. '193 patent at 49:59-62. **24(L)** There are many ways in which a PPE 650 might be compromised. The goal of the security provided by VDE 100 is to reduce the possibility that the system will be compromised, and minimize the adverse effects if it is compromised. '193 patent at 221:2-6. **24(M)** VDE 100 provided by the preferred embodiment has sufficient security to help ensure that it cannot be compromised short of a successful "brute force attack," and so that the time and cost to succeed in such a "brute force attack" substantially exceeds any value to be derived. In addition, the security provided by VDE 100 compartmentalizes the internal workings of VDE so that a successful "brute force attack" would compromise only a strictly bounded subset of protected information, not the entire system. '193 patent at 199:38-46. **24(N)** VDE supports trusted (sufficiently secure) electronic information distribution and usage control models for both commercial electronic content distribution and data security applications. '193 patent at 16:25-28. **24(O)** Employing VDE as a general purpose electronic

	Claim Term / Phrase	InterTrust Evidence
		transaction/distribution control system allows users to maintain a single transaction management control arrangement on each of their computers, networks, communication nodes, and/or other electronic appliances. Such a general purpose system can serve the needs of many electronic transaction management applications without requiring distinct, different installations for different purposes. As a result, users of VDE can avoid the confusion and expense and other inefficiencies of different, limited purpose transaction control applications for each different content and/or business model. '193 patent at 11:38-49; '900 patent at 11:36-47. --- **24(P)** [VDE features] support security techniques that materially increase the time required to "break" a system's integrity. This includes using a collection of techniques that minimizes the damage resulting from comprising some aspect of the security features of the present inventions. '193 patent at 35:59-63 --- **24(Q)** Fingerprinting electronic content before it is encrypted for transfer to a customer or other user provides information that can be very useful for identifying who received certain content which may have then been distributed or made available in unencrypted form. This information would be useful in tracking who may have "broken" the security of a VDE installation and was illegally making certain electronic content available to others. '193 patent at 38:4-12 --- **24(R)** If a content key becomes compromised, the portion of the content encrypted with the key is also compromised until the key "ages" and expires. If the "aging" process for that key also becomes compromised, then the breach becomes permanent. '193 patent at 222:49-53.

	Claim Term / Phrase	InterTrust Evidence
		24(S) If PPE 650 (or a VDE administrator watching its activities or communicating with it) detects that it has been compromised, it may be updated with an initialization to use new code, keys and new encryption/decryption algorithms. This would limit exposure to VDE objects 300 that existed at the time the encryption scheme was broken. '193 patent at 223:4-10. **Citations from Sources Designated by Microsoft under PLR 4-2(b)** **24(T)** Furthermore, there is never an absolute sense in which a system is secure or reliable. Neumann, Computer Related Risks (ACM Press, 1995), p. 2. **24(U)** The fundamental purpose of security is to minimize the risk of loss from (1) physical damage or destruction, (2) human errors and omissions, and (3) theft or unauthorized disclosure. That purpose is best fulfilled by effective loss-prevention efforts. Loss-prevention efforts involve the identification and assessment of risks to capital, human, informational, and technological assets, and the development of suitable and cost-feasible countermeasures. Hutt et al., Computer Security Handbook, 2d ed. (Macmillan, 1988), p. 75. **24(V)** Total software security is no more attainable than is perfect security in any other area. A highly skilled programmer can almost always penetrate software safeguards written by another programmer. Of course, the same can be said for attorneys; an unprincipled lawyer can usually get around protections in a contract written by an-other lawyer. Yet contracts continue to be written, and, for the most part, they are effective. Computer software security routines can also be effective most of the time. A

	Claim Term / Phrase	InterTrust Evidence
		security procedure does not have to be all-encompassing; if it provides reasonable protection at an acceptable cost, it is certainly worthwhile. The basic consideration is one of degree—how important are specific elements of data and software, and how important is their security. Some data require very little security. For example, a software library containing programs that are similar to those found in many other computer installations does not require elaborate security protection against theft. On the other hand, proprietary programs and sensitive data require extensive security. A data base containing payroll information requires stringent security procedures to maintain its confidentiality. Hutt et al., Computer Security Handbook, 2d ed. (Macmillan, 1988), p. 201. **24(W)** Regardless of which form of data storage is being considered, one must bear in mind a vital concept: no data processing installation can afford 100 percent security—if indeed there is such a thing. Hutt et al., Computer Security Handbook, 2d ed. (Macmillan, 1988), p. 218. **24(X)** One hundred percent security cannot be achieved. The most effective systems apply security protection techniques in layers. Each layer of protection diminishes the chances of someone breaking through the barriers. Hutt et al., Computer Security Handbook, 2d ed. (Macmillan, 1988), pp. 293. **24(Y)** Risk analysis is not intended to come up with a plan for absolute security. Indeed, absolute security is not achievable in today's computer's systems. Rather, risk analysis produces a degree of security commensurate with the information to be protected and with the amount of resources to be expended. Hoffman, Modern Methods for Computer Security and Privacy (Prentice-Hall, 1977), p. 170.

	Claim Term / Phrase	InterTrust Evidence
		24(Z) No matter how secure you make them, computers can always be broken into given sufficient resources, time, and money. Computers are especially vulnerable because software is complex and we don't always know if there are flaws present that make the task of breaking in easier. Even systems that are certified according to the Department of Defense's so-called Orange Book are vulnerable, especially if they are not administered correctly. Just as six-foot-thick vaults doors don't work if they're not administered properly. Garfinkel et al., Practical Unix Security (O'Reilly & Associates, 1991), pp. 13. **24(AA)** Security is a relative, not an absolute, concept, and gains in security often come only with penalties in performance. Landwehr, Formal Models for Computer Security, ACM Computer Surveys (Sept. 3, 1981), p. 253. **<u>File Histories</u>** **24(BB)** 1. Restriction to one of the following inventions is required under 35 U.S.C. § 121: Group I . . . drawn to a secure component-based operating process, classified in Classs 380, subclass 25. Group II. . . . drawn to method(s) for managing a resource or operating, classified in Class 380, subclass 4. Group III. . . . drawn to a secure method, classified in Class 380, subclass 3. Group IV. . . . drawn to [a] method of negotiating electronic contracts, classified in Class 364, subclass 401. Group V. . . . drawn to methods of auditing a resource, classified in Class 364, subclass 406.

	Claim Term / Phrase	InterTrust Evidence
		The inventions are distinct, each from the other because of the following reasons: 2. Inventions of Groups I-V are related as subcombinations disclosed as usable together in a single combination. The subcombinations are distinct from each other if they are shown to be separately usable. In the instant case, invention of Group I has separate utility such as protecting executable code from computer viruses. Invention of Group II has separate utility such as a computer network administration. Invention of Group III has separate utility such as protection of software. Invention of Group IV has separate utility such as a contract bidding procedure. Invention of Group V has separate utility such as auditing pay television . . . 3. Because these inventions are distinct for the reasons given above and have acquired a separate status in the art as shown by their different classification, restriction for examination purposes as indicated is proper. 4. Because these inventions are distinct for the reasons given above and have acquired a separate status in the art because of their recognized divergent subject matter, restriction for examination purposes as indicated is proper. '193 File History, 9/25/96 Office Action, pp. 2-3 (a complete copy of this document is attached to the Declaration of Douglas K. Derwin In Support of InterTrust's Claim Construction Position).

	Claim Term / Phrase	InterTrust Evidence
25.	193.1: "a budget specifying the number of copies which can be made of said digital file"	**Patent Specifications** **25(A)** Traveling objects can also be used to facilitate "moving" an object from one electronic appliance 600 to another. A user could move a traveling object, with its incorporated one or more permission records 808 from a desktop computer, for example, to his notebook computer. A traveling object might register its user within itself and thereafter only be useable by that one user. A traveling object might maintain separate budget information, one for the basic distribution budget record, and another for the "active" distribution budget record of the registered user. In this way, the object could be copied and passed to another potential user, and then could be a portable object for that user. '193 patent at 133:39-50. **25(B)** Meters and budgets are perhaps among the most common data structures in VDE 100. They are used to count and record events, and also to limit events. The data structures for each meter and budget are determined by the content provider or a distributor/redistributor authorized to change the information. Meters and budgets, however, generally have common information stored in a common header format (e.g., user ID, site ID and related identification information). The content provider or distributor/redistributor may specify data structures for each meter and budget UDE. Although these data structures vary depending upon the particular application, some are more common than others. The following table lists some of the more commonly occurring data structures for METER and BUDGET methods: Field type | Format | Typical Use | Description or Use Ascending Use Counter | byte, short, long, or unsigned versions of the | Meter /Budget | Ascending count of uses.

	Claim Term / Phrase	InterTrust Evidence

	same widths		
Descending Use Counter	byte, short, long, or unsigned versions of the same widths	Budget	Descending count of permitted use; eg., remaining budget.
Counter /Limit	2, 4 or 8 byte integer split into two related bytes or words	Meter /Budget	usage limits since a specific time; generally used in compound meter data structures.
Bitmap	Array bytes	Meter /Budget	Bit indicator of use or ownership.
Wide bitmap	Array of bytes	Meter /Budget	Indicator of use or ownership that may age with time.
Last Use Date	time_t	Meter /Budget	Date of last use.
Start Date	time_t	Budget	Date of first allowable use.
Expiration Date	time_t	Meter /Budget	Expiration Date.
Last Audit Date	time_t	Meter /Budget	Date of last audit.
Next Audit Date	time_t	Meter /Budget	Date of next required audit.
Auditor	VDE ID	Meter /Budget	VDE ID of authorized auditor.

The information in the table above is not complete or comprehensive, but rather is intended to show some examples of types of information that may be stored in meter and budget related data structures. The actual structure of particular meters and budgets is determined by one or more DTDs 1108 associated with

	Claim Term / Phrase	InterTrust Evidence
		the load modules 1100 that create and manipulate the data structure. A list of data types permitted by the DTD interpreter 590 in VDE 100 is extensible by properly authorized parties. '193 patent at 143:38-144:31.
		25(C) During the same or different communications exchange, the same or different clearinghouse may handle the end user's request for additional budget and/or permission pertaining to VDE object 300. For example, the end user's electronic appliance 600 may (e.g., in response to a user input request to access a particular VDE object 300) send an administrative object to the clearinghouse requesting budgets and/or other permissions allowing access (Block 1164). As mentioned above, such requests may be transmitted in the form of one or more administrative objects, such as, for example, a single administrative object having multiple "events" associated with multiple requested budgets and/or other permissions for the same or different VDE objects 300. The clearinghouse may upon receipt of such a request, check the end user's credit, financial records, business agreements and/or audit histories to determine whether the requested budgets and/or permissions should be given. The clearinghouse may, based on this analysis, send one or more responsive administrative objects which cause the end user's electronic appliance 600 to update its secure database in response (Block 1166, 1168). This updating might, for example, comprise replacing an expired PERC 808 with a fresh one, modifying a PERC to provide additional (or lesser) rights, etc. Steps 1164-1168 may be repeated multiple times in the same or different communications session to provide further updates to the end user's secure database 610. '193 patent at 162:39-65.
		25(D) In the example shown in Figure 41d, a distributor at a VDE distributor node (106) might request budget from a content creator at another node (102). This request may be made in the context of a secure VDE communication or it may be passed in an "out-of-channel" communication (e.g. a telephone call or letter). The creator 102 may decide to grant budget to the distributor 106 and

	Claim Term / Phrase	InterTrust Evidence
		processes a distribute event (1452 in BUDGET method 1510 at VDE node 102). A result of processing the distribute event within the BUDGET method might be a secure communication (1454) between VDE nodes 102 and 106 by which a budget granting use and redistribute rights to the distributor 106 may be transferred from the creator 102 to the distributor. The distributor's VDE node 106 may respond to the receipt of the budget information by processing the communication using the reply process 1475B of the BUDGET method 1510. The reply event processing 1475B might, for example, install a budget and PERC 808 within the distributor's VDE 106 node to permit the distributor to access content or processes for which access is control at least in part by the budget and/or PERC. At some point, the distributor 106 may also desire to use the content to which she has been granted rights to access. After registering to use the content object, the user 112 would be required to utilize an array of "use" processes 1476C to, for example, open, read, write, and/or close the content object as part of the use process. Once the distributor 106 has used some or all of her budget, she may desire to obtain additional budget. The distributor 106 might then initiate a process using the BUDGET method request process (1480B). Request process 1480B might initiate a communication (1482AB) with the content creator VDE node 102 requesting more budget and perhaps providing details of the use activity to date (e.g., audit trails). The content creator 102 processes the 'get more budget' request event 1482AB using the response process (1484A) within the creator's BUDGET method 1510A. Response process 1484A might, for example, make a determination if the use information indicates proper use of the content, and/or if the distributor is credit worthy for more budget. The BUDGET method response process 1484A might also initiate a financial transaction to transfer funds from the distributor to pay for said use, or use the distribute process 1472A to distribute budget to the distributor 106. A response to the distributor 106 granting more budget (or denying more budget) might be sent immediately as a response to the request communication 1482AB, or it might be sent at a later time as part of a separate communication. The response communication, upon being received at the distributor's VDE node 106, might be processed using the reply process 1475B within the distributor's copy of the BUDGET method 1510B. The reply process 1475B might then process the additional budget in the same manner as described above. The chain of handling and control may, in addition to posting

	Claim Term / Phrase	InterTrust Evidence
		budget information, also pass control information that governs the manner in which said budget may be utilized. For example, the control information specified in the above example may also contain control information describing the process and limits that apply to the distributor's redistribution of the right to use the creator's content object. Thus, when the distributor responds to a budget request from a user (a communication between a user at VDE node 112 to the distributor at VDE node 106 similar in nature to the one described above between VDE nodes 106 and 102) using the distribute process 1472B within the distributor's copy of the BUDGET method 1510B, a distribution and request/response/reply process similar to the one described above might be initiated. '193 patent at 172:61-174:29. **25(E)** Transportability of VDE Installations Between PPEs 650 In a preferred embodiment, VDE objects 300 and other secure information may, if appropriate, be transported from one PPE 650 to another securely using the various keys outlined above. VDE 100 uses redistribution of VDE administrative information to exchange ownership of VDE object 300, and to allow the portability of objects between electronic appliances 600. The permissions record 808 of VDE objects 300 contains rights information that may be used to determine whether an object can be redistributed in whole, in part, or at all. If a VDE object 300 can be redistributed, then electronic appliance 600 normally must have a "budget" and/or other permissioning that allows it to redistribute the object. For example, an electronic appliance 600 authorized to redistribute an object may create an administrative object containing a budget or rights less than or equal to the budget or rights that it owns. Some administrative objects may be sent to other PPEs 650. A PPE 650 that receives one of the administrative objects may have the ability to use at least a portion of the budgets, or rights, to related objects. '193 patent at 220:20-40.

	Claim Term / Phrase	InterTrust Evidence
		25(F) In addition, for example, an end-user of such content might be limited by the same content control information to making three copies of such content, one for each of three different computers he or she uses (one desktop computer at work, one for a desktop computer at home, and one for a portable computer). '193 patent at 48:29-35. **25(G)** . . . plural, different control models regulating the use and/or auditing of either the same specific copy of electronic information content and/or differently regulating different copies (occurrences) of the same electronic information content. Differing models for billing, auditing, and security can be applied to the same piece of electronic information content and such differing sets of control information may employ, for control purposes, the same, or differing, granularities of electronic information control increments. This includes supporting variable control information for budgeting and auditing usage as applied to a variety of predefined increments of electronic information, including employing a variety of different budgets and/or metering increments for a given electronic information deliverable for: billing units of measure, credit limit, security budget limit and security content metering increments, and/or market surveying and customer profiling content metering increments. '193 patent at 28:19-37. **25(H)** . . . support the flowing of content control information through different "branches" of content control information handling so as to accommodate, under the present invention's preferred embodiment, diverse controlled distributions of VDE controlled content. This allows different parties to employ the same initial electronic content with differing (perhaps competitive) control strategies. In this instance, a party who first placed control information on content can make certain control assumptions and these assumptions would evolve into more specific and/or extensive control assumptions. These control assumptions can evolve during the branching

	Claim Term / Phrase	InterTrust Evidence
		sequence upon content model participants submitting control information changes, for example, for use in "negotiating" with "in place" content control information. This can result in new or modified content control information and/or it might involve the selection of certain one or more already "in-place" content usage control methods over in-place alternative methods, as well as the submission of relevant control information parameter data. This form of evolution of different control information sets applied to different copies of the same electronic property content and/or appliance results from VDE control information flowing "down" through different branches in an overall pathway of handling and control and being modified differently as it diverges down these different pathway branches. '193 patent at 31:29-56. **25(I)** . . . multiple simultaneous control models for the same content property and/or property portion. This allows, for example, for concurrent business activities which are dependent on electronic commercial product content distribution, such as acquiring detailed market survey information and/or supporting advertising, both of which can increase revenue and result in lower content costs to users and greater value to content providers. Such control information and/or overall control models may be applied, as determined or allowed by control information, in differing manners to different participants in a pathway of content, reporting, payment, and/or related control information handling. VDE supports applying different content control information to the same and/or different content and/or appliance usage related activities, and/or to different parties in a content and/or appliance usage model, such that different parties (or classes of VDE users, for example) are subject to differing control information managing their use of electronic information content. For example, differing control models based on the category of a user as a distributor of a VDE controlled content object or an end-user of such content may result in different budgets being applied. Alternatively, for example, a one distributor may have the right to distribute a different array of properties than another distributor (from a common content collection provided, for example, on optical disc). An individual, and/or a class or other grouping of end-users, may have different costs (for example, a student, senior citizen, and/or poor citizen user of content who may

	Claim Term / Phrase	InterTrust Evidence
		be provided with the same or differing discounts) than a "typical" content user. '193 patent at 30:42-31:7. **25(J)** Such different application of control information may also result from content control information specifying that a certain party or group of parties shall be subject to content control information that differs from another party or group of parties. For example, content control information for a given piece of content may be stipulated as senior information and therefore not changeable, might be put in place by a content creator and might stipulate that national distributors of a given piece of their content may be permitted to make 100,000 copies per calendar quarter, so long as such copies are provided to bona fide end-users, but may pass only a single copy of such content to a local retailers and the control information limits such a retailer to making no more than 1,000 copies per month for retail sales to end-users. In addition, for example, an end-user of such content might be limited by the same content control information to making three copies of such content, one for each of three different computers he or she uses (one desktop computer at work, one for a desktop computer at home, and one for a portable computer). '193 patent at 48:15-35. **25(K)** In this example, as illustrated in Figure 80, user B may receive control information associated with creator A's content from distributor A and/or user/distributor B. In either case, user B may be able to establish their own control information on DA(CA) and/or UDB(UDA(DA(CA))), respectively (if allowed by such control information. The resulting set(s) of control information UB(DA(CA)) and/or UB(UDB(UDA(DA(CA)))) respectively, may represent different control scenarios, each of which may have benefits for user B. As described in connection with an earlier example, user B may have received control information from user/distributor B along a chain of handling including user/distributor A that bases fees on the number of minutes that user B makes use of creator A's content (and requiring user/distributor A

	Claim Term / Phrase	InterTrust Evidence
		to pay fees of $15 per month per user to distributor A regardless of the amount of usage by user B in a calendar month). This may be more favorable under some circumstances than the fees required by a direct use of control information provided by distributor A, but may also have the disadvantage of an exhausted chain of redistribution and, for example, further usage information reporting requirements included in UDB(UDA(DA(CA))). If the two sets of control information DA(CA) and UDB(UDA(DA(CA))) permit (e.g. do not require exclusivity enforced, for example, by using a registration interval in an object registry used by a secure subsystem of user B's VDE installation to prevent deregistration and reregistration of different sets of control information related to a certain container (or registration of plural copies of the same content having different control information and/or being supplied by different content providers) within a particular interval of time as an aspect of an extended agreement for a chain of handling and control reflected in DA(CA) and/or UDB(UDA(DA(CA)))), user B may have both sets of control information registered and may make use of the set that they find preferable under a given usage scenario. '193 patent at 306:30-65. **25(L)** For example, user/distributor A may receive control information CB that includes a requirement that user/distributor A pay creator B for content decrypted by user/distributor A (and any participant receiving distributed and/or redistributed control information from user/distributor A) at the rate of $0.50 per kilobyte. As indicated above, user/distributor A also may receive control information associated with creator B's VDE content container from distributor A. In this example, user/distributor A may have a choice between paying a "rental" fee through a chain of handling passing through distributor A, and a fee based on the quantity of decryption through a chain of handling direct to creator B. In this case, user/distributor A may have the ability to choose to use either or both of CB and DA(CB). '193 patent at 308:29-42. **25(M)** As illustrated in Figure 81, in this example, user B may receive

	Claim Term / Phrase	InterTrust Evidence
		control information associated with creator B's VDE content container from six different sources: CB directly from creator B, DA(CB) from distributor A, UDB(UDA(DA(CB))) and/or UDB(UDA(CB)) from user/distributor B, DC(CB) from distributor C, and/or DB(DC(CB)) from distributor B. This represents six chains of handling through which user B may enter into extended agreements with other participants in this example. Two of these chains pass through user/distributor B. Based on a VDE negotiation between user/distributor B and user B, an extended agreement may be reached (if permitted by control information governing both parties) that reflects the conditions under which user B may use one or both sets of control information. In this example, two chains of handling and control may "converge" at user/distributor B, and then pass to user B (and if control information permits, later diverge once again based on distribution and/or redistribution by user B). '193 patent at 308:48-65. **25(N)** User B may, in this example, receive a VDE content container from distributor C that is comprised of VDE objects created by creator B, creator C, and creator D. In addition, user B may receive a VDE content container from distributor B that contains the same content created by creator B, creator C, and creator D in addition to one or more extracted/embedded portions of content created by creator E. User B may base decisions concerning which of such containers they choose to use (including which embedded containers she may wish to use), and under which circumstances, based on, for example, the character of such extracted/embedded portions (e.g. multimedia presentations illustrating potential areas of interest in the remainder of the content, commentary explaining and/or expositing other elements of content, related works, improved application software delivered as an element of content, etc.); the quality, utility, and/or price (or other attributes of control information) of such portions; and other considerations which distinguish the containers and/or content control information received, in this example, from distributor B and distributor C. '193 patent at 312:11-31.

	Claim Term / Phrase	InterTrust Evidence
		25(O) As with standard VDE objects 300, a user may be required to contact a clearinghouse service to acquire additional budgets if the user wishes to continue to use the traveling object after the exhaustion of an available budget(s) . . . . '193 patent at 131:10-13. **25(P)** Once the distributor 106 has used some or all of her budget, she may desire to obtain additional budget. The distributor 106 might then initiate a process using the BUDGET method request process (1480B). Request process 1480B might initiate a communication (1482AB) with the content creator VDE node 102 requesting more budget and perhaps providing details of the use activity to date (e.g., audit trails). The content creator 102 processes the 'get more budget' request event 1482AB using the response process (1484A) within the creator's BUDGET method 1510A. Response process 1484A might, for example, make a determination if the use information indicates proper use of the content, and/or if the distributor is credit worthy for more budget. The BUDGET method response process 1484A might also initiate a financial transaction to transfer funds from the distributor to pay for said use, or use the distribute process 1472A to distribute budget to the distributor 106. A response to the distributor 106 granting more budget (or denying more budget) might be sent immediately as a response to the request communication 1482AB, or it might be sent at a later time as part of a separate communication. The response communication, upon being received at the distributor's VDE node 106, might be processed using the reply process 1475B within the distributor's copy of the BUDGET method 1510B. The reply process 1475B might then process the additional budget in the same manner as described above. '193 patent at 173:21-174:14. **25(Q)** During the same or different communications exchange, the same or different clearinghouse may handle the end user's request for additional budget and/or permission pertaining to VDE object 300.

	Claim Term / Phrase	InterTrust Evidence
		For example, the end user's electronic appliance 600 may (e.g., in response to a user input request to access a particular VDE object 300) send an administrative object to the clearinghouse requesting budgets and/or other permissions allowing access (Block 1164). As mentioned above, such requests may be transmitted in the form of one or more administrative objects, such as, for example, a single administrative object having multiple "events" associated with multiple requested budgets and/or other permissions for the same or different VDE objects 300. The clearinghouse may upon receipt of such a request, check the end user's credit, financial records, business agreements and/or audit histories to determine whether the requested budgets and/or permissions should be given. The clearinghouse may, based on this analysis, send one or more responsive administrative objects which cause the end user's electronic appliance 600 to update its secure database in response (Block 1166, 1168). This updating might, for example, comprise replacing an expired PERC 808 with a fresh one, modifying a PERC to provide additional (or lesser) rights, etc. Steps 1164-1168 may be repeated multiple times in the same or different communications session to provide further updates to the end user's secure database 610. '193 patent at 162:39-65.

	Claim Term / Phrase	InterTrust Evidence
26.	193.1: "controlling the copies made of said digital file"	**<u>Patent Specifications</u>** **26(A)** . . . plural, different control models regulating the use and/or auditing of either the same specific copy of electronic information content and/or differently regulating different copies (occurrences) of the same electronic information content. Differing models for billing, auditing, and security can be applied to the same piece of electronic information content and such differing sets of control information may employ, for control purposes, the same, or differing, granularities of electronic information control increments. This includes supporting variable control information for budgeting and auditing usage as applied to a variety of predefined increments of electronic information, including employing a variety of different budgets and/or metering increments for a given electronic information deliverable for: billing units of measure, credit limit, security budget limit and security content metering increments, and/or market surveying and customer profiling content metering increments. '193 patent at 28:19-37. **26(B)** . . . support the flowing of content control information through different "branches" of content control information handling so as to accommodate, under the present invention's preferred embodiment, diverse controlled distributions of VDE controlled content. This allows different parties to employ the same initial electronic content with differing (perhaps competitive) control strategies. In this instance, a party who first placed control information on content can make certain control assumptions and these assumptions would evolve into more specific and/or extensive control assumptions. These control assumptions can evolve during the branching sequence upon content model participants submitting control information changes, for example, for use in "negotiating" with "in place" content control information. This can result in new or modified content control information and/or it might involve the selection of certain one or more already "in-place" content usage control methods over in-place alternative methods, as well as the submission of relevant control information parameter data. This form of evolution of different control information sets applied to different copies of the same electronic property content and/or

	Claim Term / Phrase	InterTrust Evidence
		appliance results from VDE control information flowing "down" through different branches in an overall pathway of handling and control and being modified differently as it diverges down these different pathway branches. '193 patent at 31:29-56. **26(C)** . . . multiple simultaneous control models for the same content property and/or property portion. This allows, for example, for concurrent business activities which are dependent on electronic commercial product content distribution, such as acquiring detailed market survey information and/or supporting advertising, both of which can increase revenue and result in lower content costs to users and greater value to content providers. Such control information and/or overall control models may be applied, as determined or allowed by control information, in differing manners to different participants in a pathway of content, reporting, payment, and/or related control information handling. VDE supports applying different content control information to the same and/or different content and/or appliance usage related activities, and/or to different parties in a content and/or appliance usage model, such that different parties (or classes of VDE users, for example) are subject to differing control information managing their use of electronic information content. For example, differing control models based on the category of a user as a distributor of a VDE controlled content object or an end-user of such content may result in different budgets being applied. Alternatively, for example, a one distributor may have the right to distribute a different array of properties than another distributor (from a common content collection provided, for example, on optical disc). An individual, and/or a class or other grouping of end-users, may have different costs (for example, a student, senior citizen, and/or poor citizen user of content who may be provided with the same or differing discounts) than a "typical" content user. '193 patent at 30:42-31:7. **26(D)** Such different application of control information may also result from content control information specifying that a certain party or

	Claim Term / Phrase	InterTrust Evidence
		group of parties shall be subject to content control information that differs from another party or group of parties. For example, content control information for a given piece of content may be stipulated as senior information and therefore not changeable, might be put in place by a content creator and might stipulate that national distributors of a given piece of their content may be permitted to make 100,000 copies per calendar quarter, so long as such copies are provided to bona fide end-users, but may pass only a single copy of such content to a local retailers and the control information limits such a retailer to making no more than 1,000 copies per month for retail sales to end-users. In addition, for example, an end-user of such content might be limited by the same content control information to making three copies of such content, one for each of three different computers he or she uses (one desktop computer at work, one for a desktop computer at home, and one for a portable computer). '193 patent at 48:15-35. **26(E)** In this example, as illustrated in Figure 80, user B may receive control information associated with creator A's content from distributor A and/or user/distributor B. In either case, user B may be able to establish their own control information on DA(CA) and/or UDB(UDA(DA(CA))), respectively (if allowed by such control information. The resulting set(s) of control information UB(DA(CA)) and/or UB(UDB(UDA(DA(CA)))) respectively, may represent different control scenarios, each of which may have benefits for user B. As described in connection with an earlier example, user B may have received control information from user/distributor B along a chain of handling including user/distributor A that bases fees on the number of minutes that user B makes use of creator A's content (and requiring user/distributor A to pay fees of $15 per month per user to distributor A regardless of the amount of usage by user B in a calendar month). This may be more favorable under some circumstances than the fees required by a direct use of control information provided by distributor A, but may also have the disadvantage of an exhausted chain of redistribution and, for example, further usage information reporting requirements included in UDB(UDA(DA(CA))). If the two sets of control information DA(CA) and UDB(UDA(DA(CA))) permit (e.g. do not require exclusivity enforced, for example, by using a registration interval in an object registry used by a secure subsystem of user B's VDE installation to prevent deregistration and

	Claim Term / Phrase	InterTrust Evidence
		built to execute only in SPE 503 secure space for government classes of security, or in an HPE 655 for commercial applications. As described above, the load module public header 802 may contain an "execution space code" field that indicates where the load module 1100 needs to execute. '193 patent at 140:15-46.

	Claim Term / Phrase	InterTrust Evidence
		reregistration of different sets of control information related to a certain container (or registration of plural copies of the same content having different control information and/or being supplied by different content providers) within a particular interval of time as an aspect of an extended agreement for a chain of handling and control reflected in DA(CA) and/or UDB(UDA(DA(CA)))), user B may have both sets of control information registered and may make use of the set that they find preferable under a given usage scenario. '193 patent at 306:30-65. **26(F)** For example, user/distributor A may receive control information CB that includes a requirement that user/distributor A pay creator B for content decrypted by user/distributor A (and any participant receiving distributed and/or redistributed control information from user/distributor A) at the rate of $0.50 per kilobyte. As indicated above, user/distributor A also may receive control information associated with creator B's VDE content container from distributor A. In this example, user/distributor A may have a choice between paying a "rental" fee through a chain of handling passing through distributor A and a fee based on the quantity of decryption through a chain of handling direct to creator B. In this case, user/distributor A may have the ability to choose to use either or both of CB and DA(CB). '193 patent at 308:29-42. **26(G)** As illustrated in Figure 81, in this example, user B may receive control information associated with creator B's VDE content container from six different sources: CB directly from creator B, DA(CB) from distributor A, UDB(UDA(DA(CB))) and/or UDB(UDA(CB)) from user/distributor B, DC(CB) from distributor C, and/or DB(DC(CB)) from distributor B. This represents six chains of handling through which user B may enter into extended agreements with other participants in this example. Two of these chains pass through user/distributor B. Based on a VDE negotiation between user/distributor B and user B, an extended agreement may be reached (if permitted by control information governing both parties) that reflects the conditions under which user B may use one

	Claim Term / Phrase	InterTrust Evidence
		or both sets of control information. In this example, two chains of handling and control may "converge" at user/distributor B, and then pass to user B (and if control information permits, later diverge once again based on distribution and/or redistribution by user B). '193 patent at 308:48-65. **26(H)** User B may, in this example, receive a VDE content container from distributor C that is comprised of VDE objects created by creator B, creator C, and creator D. In addition, user B may receive a VDE content container from distributor B that contains the same content created by creator B, creator C, and creator D in addition to one or more extracted/embedded portions of content created by creator E. User B may base decisions concerning which of such containers they choose to use (including which embedded containers she may wish to use), and under which circumstances, based on, for example, the character of such extracted/embedded portions (e.g. multimedia presentations illustrating potential areas of interest in the remainder of the content, commentary explaining and/or expositing other elements of content, related works, improved application software delivered as an element of content, etc.); the quality, utility, and/or price (or other attributes of control information) of such portions; and other considerations which distinguish the containers and/or content control information received, in this example, from distributor B and distributor C. '193 patent at 312:11-31.

	Claim Term / Phrase	InterTrust Evidence
27.	721.1: "digitally signing a second load module with a second digital signature different from the first digital signature, the second digital signature designating the second load module for use by a second device class having at least one of tamper resistance and security level different from the at least one of tamper resistance and security level of the first device class"	**<u>Patent Specifications</u>** **27(A)** In accordance with one aspect provided by the present invention, one or more trusted verifying authorities validate load modules or other executables by analyzing and/or testing them. A verifying authority digitally "signs" and "certifies" those load modules or other executables it has verified (using a public key based digital signature and/or certificate based thereon, for example). Protected execution spaces such as protected processing environments can be programmed or otherwise conditioned to accept only those load modules or other executables bearing a digital signature/certificate of an accredited (or particular) verifying authority. '721 patent at 4:61-5:5. --- **27(B)** A hierarchy of assurance levels may be provided for different protected processing environment security levels. Load modules or other executables can be provided with digital signatures associated with particular assurance levels. Appliances assigned to particular assurance levels can protect themselves from executing load modules or other executables associated with different assurance levels. Different digital signatures and/or certificates may be used to distinguish between load modules or other executables intended for different assurance levels. This strict assurance level hierarchy provides a framework to help ensure that a more trusted environment can protect itself from load modules or other executables exposed to environments with different work factors (e.g., less trusted or tamper resistant environments). This can be used to provide a high degree of security compartmentalization that helps protect the remainder of the system should parts of the system become compromised. For example, protected processing environments or other secure execution spaces that are more impervious to tampering (such as those providing a higher degree of physical security) may use an assurance level that isolates it from protected processing environments or other secure execution spaces that are relatively more susceptible to tampering (such as those constructed solely by software executing on a general purpose digital computer in a non-

	Claim Term / Phrase	InterTrust Evidence
		secure location). A verifying authority may digitally sign load modules or other executables with a digital signature that indicates or implies assurance level. A verifying authority can use digital signature techniques to distinguish between assurance levels. As one example, each different digital signature may be encrypted using a different verification key and/or fundamentally different encryption, one-way hash and/or other techniques. A protected processing environment or other secure execution space protects itself by executing only those load modules or other executables that have been digitally signed for its corresponding assurance level. The present invention may use a verifying authority and the digital signatures it provides to compartmentalize the different electronic appliances depending on their level of security (e.g., work factor or relative tamper resistance). In particular, a verifying authority and the digital signatures it provides isolate appliances with significantly different work factors — preventing the security of high work factor appliances from collapsing into the security of low work factor appliances due to free exchange of load modules or other executables. '721 patent at 6:16-62. **27(C)** Figures 11A-11C show how a verifying authority can use different digital signatures to designate the same or different load modules as being appropriate for execution by different assurance level electronic appliances; Figures 12, 13 and 13A show how assurance level digital signatures can be used to isolate electronic appliances or appliance types based on work factor and/or tamper resistance to reduce overall security risks; '721 patent at 7:66-8:6.

	Claim Term / Phrase	InterTrust Evidence
		27(D) Assurance Levels Verifying authority 100 can use different digital signing techniques to provide different "assurance levels" for different kinds of electronic appliances 61 having different "work factors" or levels of tamper resistance. Figures 10A-10C show an example assurance level hierarchy providing three different assurance levels for different electronic appliance types: Assurance level I might be used for an electronic appliance(s) 61 whose protected processing environment 108 is based on software techniques that may be somewhat resistant to tampering. An example of an assurance level I electronic appliance 61A might be a general purpose personal computer that executes software to create protected processing environment 108. An assurance level II electronic appliance 61B may provide a protected processing environment 108 based on a hybrid of software security techniques and hardware-based security techniques. An example of an assurance level II electronic appliance 61B might be a general purpose personal computer equipped with a hardware integrated circuit secure processing unit ("SPU") that performs some secure processing outside of the SPU (see Ginter et al. patent disclosure Figure 10 and associated text). Such a hybrid arrangement might be relatively more resistant to tampering than a software-only implementation. The assurance level III appliance 61C shown is a general purpose personal computer equipped with a hardware-based secure processing unit 132 providing and completely containing protected processing environment 108 (see Ginter et al. Figures 6 and 9 for example). A silicon-based special purpose integrated circuit security chip is relatively more tamper-resistant than implementations relying on software techniques for some or all of their tamper-resistance. In this example, verifying authority 100 digitally signs load modules 54 using different digital signature techniques (for example, different "private" keys 122) based on assurance level. The digital signatures 106 applied by verifying authority 100 thus securely encode the same (or different) load module 54 for use by appropriate corresponding assurance level electronic appliances 61. Assurance level in this example may be assigned to a particular

	Claim Term / Phrase	InterTrust Evidence
		protected processing environment 108 at initialization (e.g., at the factory in the case of hardware-based secure processing units). Assigning assurance level at initialization time facilitates the use of key management (e.g., secure key exchange protocols) to enforce isolation based on assurance level. For example, since establishment of assurance level is done at initialization time, rather than in the field in this example, the key exchange mechanism can be used to provide new keys (assuming an assurance level has been established correctly). '721 patent at 16:37-17:23. --- **27(E)** In one example, verifying authority 100 may digitally sign identical copies of load module 54 for use by different classes or "assurance levels" of electronic appliances 61. If the sharing of a load module 54 between different electronic appliances is regarded as an open communications channel between the protected processing environments 108 of the two appliances, it becomes apparent that there is a high degree of risk in permitting such sharing to occur. In particular, the extra security assurances and precautions of the more trusted environment are collapsed into the those of the less trusted environment because an attacker who compromises a load module within a less trusted environment is then be able to launch the same load module to attack the more trusted environment. Hence, although compartmentalization based on encryption and key management can be used to restrict certain kinds of load modules 54 to execute only on certain types of electronic appliances 61, a significant application in this context is to compartmentalize the different types of electronic appliances and thereby allow an electronic appliance to protect itself against load modules 54 of different assurance levels. '721 patent at 18:19-38. --- **27(F)** In accordance with this feature of the invention, verifying authority 100 supports all of these various categories of digital signatures, and system 50 uses key management to distribute the appropriate verification keys to different assurance level devices. For example, verifying authority 100 may digitally sign a particular load module

	Claim Term / Phrase	InterTrust Evidence
		54 such that only hardware-only based server(s) 402(3) at assurance level XI may authenticate it. This compartmentalization prevents any load module executable on hardware-only servers 402(3) from executing on any other assurance level appliance (for example, software-only protected processing environment based support service 404(1)). To simplify key management and distribution, execution environments having significantly similar work factors can be classified in the same assurance level. Figure 13 shows one example hierarchical assurance level arrangement. In this example, less secure "software only" protected processing environment 108 devices are categorized as assurance level I, somewhat more secure "software and hardware hybrid" protected processing environment appliances are categorized as assurance level II, and more trusted "hardware only" protected processing environment devices are categorized as assurance level III. '721 patent at 19:11-32. **27(G)** A load module or other executable may be certified for multiple assurance levels. Different digital signatures may be used to certify the same load module or other executable for different respective assurance levels. '721 patent at 20:1-4.

	Claim Term / Phrase	InterTrust Evidence
28.	891.1: "securely applying, at said first appliance through use of said at least one resource said first entity's control and said second entity's control to govern use of said data item"	**<u>Patent Specifications</u>** **28(A)** The embedding processes for all VDE embedded content containers normally involves securely identifying the appropriate content control information for the embedded content. For example, VDE content control information for a VDE installation and/or a VDE content container may securely, and transparently to an embedder (user), apply the same content control information to edited (such as modified or additional) container content as is applied to one or more portions (including all, for example) of previously "in place" content of said container and/or securely apply control information generated through a VDE control information negotiation between control sets, and/or it may apply control information previously applied to said content. Application of control information may occur regardless of whether the edited content is in a parent or embedded container. This same capability of securely applying content control information (which may be automatically and/or transparently applied), may also be employed with content that is embedded into a VDE container through extracting and embedding content, or through the moving, or copying and embedding, of VDE container objects. Application of content control information normally occurs securely within one or more VDE secure sub-system PPEs 650. This process may employ a VDE template that enables a user, through easy to use GUI user interface tools, to specify VDE content control information for certain or all embedded content, and which may include menu driven, user selectable and/or definable options, such as picking amongst alternative control methods (e.g. between different forms of metering) which may be represented by different icons picturing (symbolizing) different control functions and apply such functions to an increment of VDE secured content, such as an embedded object listed on an object directory display. '193 patent at 299:19-51. **28(B)** Embedded content (and/or content objects) may have been contributed by different parties and may be integrated into a VDE container through a VDE content and content control information integration process securely managed through the use of one or more secure VDE subsystems. This process may, for example, involve one or more of:

	Claim Term / Phrase	InterTrust Evidence
		(1.) securely applying instructions controlling the embedding and/or use of said submitted content, wherein said instructions were securely put in place, at least in part, by a content provider and/or user of said VDE container. For example, said user and/or provider may interact with one or more user interfaces offering a selection of content embedding and/or control options (e.g. in the form of a VDE template). Such options may include which, and/or whether, one or more controls should be applied to one or more portions of said content and/or the entry of content control parameter data (such a time period before which said content may not be used, cost of use of content, and/or pricing discount control parameters such as software program suite sale discounting). Once required and/or optional content control information is established by a provider and/or user, it may function as content control information which may be, in part or in full, applied automatically to certain, or all, content which is embedded in a VDE content container. '193 patent at 300:6-30.
		28(C) Users of VDE may include content creators who apply content usage, usage reporting, and/or usage payment related control information to electronic content and/or appliances for users such as end-user organizations, individuals, and content and/or appliance distributors. '193 patent at 9:40-45.
		28(D) For example, in a VDE aware word processor application, a user may be able to "print" a document into a VDE content container object, applying specific control information by selecting from amongst a series of different menu templates for different purposes (for example, a confidential memo template for internal organization purposes may restrict the ability to "keep," that is to make an electronic copy of the memo). '193 patent at 26:59-67.

	Claim Term / Phrase	InterTrust Evidence
		28(E) VDE supports applying different content control information to the same and/or different content and/or appliance usage related activities, and/or to different parties in a content and/or appliance usage model, such that different parties (or classes of VDE users, for example) are subject to differing control information managing their use of electronic information content. For example, differing control models based on the category of a user as a distributor of a VDE controlled content object or an end-user of such content may result in different budgets being applied. '193 patent at 30:55-65.
		28(F) Keys and tags may be securely generated within SPE 503 (HPE 655) in the preferred embodiment. '193 patent at 120:15-16.
		28(G) Frequently, for a VDE application for a given content model (such as distribution of entertainment on CD-ROM, content delivery from an Internet repository, or electronic catalog shopping and advertising, or some combination of the above) participants would be able to securely select from amongst available, alternative control methods and apply related parameter data, wherein such selection of control method and/or submission of data would constitute their "contribution" of control information. '193 patent at 18:60-19:1.
		28(H) ROS 602 assembles these elements together into an executable component assembly 690 prior to loading and executing the component assembly (e.g., in a secure operating environment such as SPE 503 and/or HPE 655). '193 patent at 83:44-48

	Claim Term / Phrase	InterTrust Evidence
29.	900.155: "derives information from one or more aspects of said host processing environment"	**<u>Patent Specifications</u>** **29(A)** Correspondence Between Installed Software and Appliance "Signature". Another technique that may be used during the installation routine 3470 is to customize the operational materials 3472 by embedding a "machine signature" into the operational materials to establish a correspondence between the installed software on a particular electronic appliance 600 (Figure 69C, block 3470(7)). This technique prevents a software-based PPE 650 from being transferred from one electronic appliance 600 to another (except through the use of the appropriate secure, verified backup mechanism). For electronic appliances 600 where it is feasible to do so, the installation procedure 3470 may determine unique information about the electronic appliance 600 (e.g., a "signature" SIG in the sense of a unique value - not necessarily a "digital signature" in the cryptographic sense). Installation routine 3470 embeds the electronic appliance "signature" SIG in the installed operational materials 3472. Upon initialization, the operational materials 3472 validate the embedded signature value against the actual electronic appliance 600 signature SIG, and may refuse to start if the comparison fails. Depending on the configuration of electronic appliance 600, the machine signature may consist, for example, of some combination of a hash of the ROM BIOS 658 (see Figure 69G), a hash of a disk defect map 3497a, the Ethernet (or other) network adapter 666 address, information written into an unused disk sector, information stored in a non-volatile CMOS RAM (such as used for hardware configuration data), information stored in non-volatile ("flash") memory (such as used for system or peripheral component "BIOS" programs) and/or hidden unique information placed into the root directory 3497b of the fixed disk drive 668.

	Claim Term / Phrase	InterTrust Evidence
		Figure 69G shows an example of some of these appliance-specific signatures. '900 patent at 239:4-42.

<table>
<tr><th></th><th>Claim Term / Phrase</th><th>InterTrust Evidence</th></tr>
<tr><td>30.</td><td>912.8:
“identifying at least one aspect of an execution space required for use and/or execution of the load module”</td><td>

<u>Patent Specifications</u>
30(A)
The following is an example of a possible field layout for load module public header 802:

<table>
<tr><th>Field Type</th><th></th><th>Description</th></tr>
<tr><td>LM ID</td><td></td><td>VDE ID of Load Module.</td></tr>
<tr><td></td><td>Creator ID</td><td>Site ID of creator of this load module.</td></tr>
<tr><td></td><td>Type ID</td><td>Constant indicates load module type.</td></tr>
<tr><td></td><td>LM ID</td><td>Unique sequence number for this load module, which uniquely identifies the load module in a sequence of load modules created by an authorized VDE participant.</td></tr>
<tr><td></td><td>Version ID</td><td>Version number of this load module.</td></tr>
<tr><td>Other classification information</td><td>Class ID</td><td>ID to support different load module classes.</td></tr>
<tr><td></td><td>Type ID</td><td>ID to support method type compatible searching.</td></tr>
<tr><td>Descriptive Information</td><td>Description</td><td>Textual description of the load module.</td></tr>
<tr><td></td><td>Execution space code</td><td>Value that describes what execution space (e.g., SPE or HPE) this load module.</td></tr>
</table>

Many load modules 1100 contain code that executes in an SPE 503. Some load modules 1100 contain code that executes in an HPE 655. This allows methods 1000 to execute in whichever environment is appropriate. For example, an INFORMATION method 1000 can be built to execute only in SPE 503 secure space for government classes of security, or in an HPE 655 for commercial applications. As described above, the load module public header 802 may contain an "execution space code" field that indicates where the load module 1100 needs to execute.

‘193 patent at 140:15-46.</td></tr>
</table>

EXHIBIT D
PLR 4-3(b) – Microsoft's Listing of Intrinsic and Extrinsic Evidence

Set forth below are references to the "instrinsic" and "extrinsic" evidence on which Microsoft may rely to support its claim construction for the 30 designated "Mini-Markman" terms and phrases. Each claim phrase incorporates the intrinsic and extrinsic support of the individual terms within it.

For ease of reference, the full titles of various intrinsic and extrinsic evidence sources are abbreviated. A key to the abbreviations is contained in Appendix 1, located at the last page of this Exhibit.

	Claim Term/Phrase	Evidence Supporting MS Construction
1.	aspect 683.2 861.58 900.155 912.8	**Intrinsic:** 1. "For each site, the manufacturer generates a site ID 2821 and list of site characteristics 2822." ('193 209:55-57) 2. See also support listed in item #29 ('900:155) **Extrinsic:** 1. Aspect: "The qualification of a descriptor." (IBM)
2.	authentication 193.15	**Intrinsic:** 1. "A certification key pair may be used as part of a 'certification' process for PPEs 650 and VDE electronic appliances 600. This certification process in the preferred embodiment may be used to permit a VDE electronic appliance to present one or more 'certificates' authenticating that it (or its key) can be trusted. As described above, this 'certification' process may be used by one PPE 650 to 'certify' that it is an authentic VDE PPE, it has a certain level of security and capability set (e.g., it is hardware based rather than merely software based), etc." ('193 212:66 - 213:15) 2. "One of the functions SPU 500 may perform is to validate/authenticate VDE objects 300 and other items. Validation/authentication often involves comparing long data strings to determine whether they compare in a predetermined way." ('193 67:56-60) 3. "Sender 4052 may select different ways to identify recipients 4056 based on the confidentiality of the document and the level of security the sender is willing to pay for. In one example, sender 4052 might require the recipient's appliance 600B to require recipient 4056 to prove that he is who he says he is. This secure 'authentication' function might be met by, for example, requiring recipient 4056 to input a password, present digital proof of identity..." ('683 17:20-27) 4. "In order to further assure the authenticity of the communication, a secure communications link may be established using a key exchange technique (e.g., Diffie-Hellman) and encryption of the signal between the stations." ('683 52:56-60) 5. "This 'channel 0' 'open channel' task may then issue a series of requests to secure database manager 566 to obtain the 'blueprint' for constructing one or more component assemblies 690 to be associated with channel 594 (block 1127). In the preferred embodiment, this 'blueprint' may comprise a PERC 808 and/or URT 464. In may be obtained by using the 'Object, User, Right' parameters passed to the 'open channel' routine to 'chain' together object registration table

	Claim Term/Phrase	Evidence Supporting MS Construction
		460 records, user/object table 462 records, URT 464 records, and PERC 808 records. This 'open channel' task may preferably place calls to key and tag manager 558 to validate and correlate the tags associated with these various records to ensure that they are authentic and match. The preferred embodiment process then may write appropriate information to channel header 596 (block 1129)." ('193 112:46-61) **Extrinsic:** 1. Authentication: "1. In computer security, verification of the identity of a user or the user's eligibility to access an object. 2. In computer security, verification that a message has not been altered or corrupted. 3. In computer security, a process used to verify the user of an information system or protected resources. 4. A process that checks the integrity of an entity." (IBM) 2. Authentication: "1. In data security, the act of determining that a message has not been changed since leaving its point of origin. ... 4. In computer security, the act of identifying or verifying the eligibility of a station, originator, or individual to access specific categories of information." (Longley)
3.	budget 193.1	**Intrinsic:** 1. "'Budgets' 308 shown in FIG. 5B are a special type of 'method' 1000 that may specify, among other things, limitations on usage of information content 304, and how usage will be paid for. Budgets 308 can specify, for example, how much of the total information content 304 can be used and/or copied. The methods 310 may prevent use of more than the amount specified by a specific budget." ('193 59:19-25) (See also Fig. 5B) 2. "For example, consider the case of a security budget. One form of a typical budget might limit the user to 10Mb of decrypted data per month." ('193 265:9-11) 3. "An example of the process steps used for the move of a budget record might look something like this: 1) Check the move budget (e.g., to determine the number of moves allowed)" ('193 265:24-27) 4. "BUDGET method 408 may store budget information in a budget UDE..." ('193 182:25-26) 5. "BUDGET method 408 may result in a 'budget remaining' field in a budget UDE being decremented by an amount specified by BILLING method 406." ('193 182:27-30) 6. "In the preferred embodiment, a 'method' 1000 is a collection of basic instructions, and information related to basic instructions, that provides context, data, requirements and/or relationships for use in performing, and/or preparing a perform, basic instructions in relation to the operation of one or more electronic appliances 600." ('193 85:43-48; see also '193 136:20-25) 7. "Budget process 408 limits how much content usage is permitted. For example, budget process 408 may limit the number of times content may be accessed or copied, or it may limit the number of pages or other amount of content that can be used based on, -for example, the number of dollars available in a credit account. Budget process 408 records and reports financial and other transaction information associated with such limits." ('193 58:27-34)

	Claim Term/Phrase	Evidence Supporting MS Construction
		8. "BUDGET method 1510 may next perform a billing operation by adding a billing amount to a budget value (block 1602)." ('193 187:48-50) 9. "The permissions and/or methods (i.e., budgets) carried by the portable appliance 2600 may have been assigned to it in conjunction with an 'encumbering' of another, stationary or other portable VDE electronic appliance 600." ('193 235:39-42) 10. "Fields used for budget (but not for meter): 'Descending use counter … Start date'" ('193 143:63 - 144:14) 11. "A budget may be specified in dollars, deutsche marks, yen, and/or in any other monetary or content measurement schema and/or organization. The preferred embodiment output of the application, normally has three basic elements. A notation in the distribution portion of secure database 610 for each budget record created, the actual budget records, and a method option record for inclusion in a permissions record." ('193 265:44-51) **Extrinsic:** 1. Budget: "A budget is the control mechanism for a meterable feature. A budget provides an upper limit for the volume of a meterable feature that a user (client) may use. Budgets consist of two values: a ceiling limit on use and an increment value that is added to the associated meter when a meterable event occurs. Budgets may be stand-alone or cascaded. A stand-alone budget only increments the meters for itself, while a cascaded budget can increment many meters from a single meterable event. A budget consists of an identification sextet, a descriptive area that describes the budget (cascade budget tuple and other miscellaneous flags), and a series of budget tuples. Each budget tuple consists of a budget and the increment value. It should be noted that a budget may be specified in meterable events or in dollars, based on the type of meter the budget will be compared against." (VDE ROI Device v1.0a, 2/9/94, IT00008582) 2. Budget Object: "A governed element that defines the consumer's ability to provide payment using a specific payment type." (IT Glossary[1], 1997-1998, ML00012B) 3. Budget Object: "*An InterTrust system object* that defines the consumer's ability to provide payment using a specific payment type." (emphasis added) (IT System Developers Kit, 1997, TD00298C) 4. Budget: "A control mechanism that limits operations on content based on billed amounts that can maintain a budget trail. A budget may be financially based (e.g., a number of dollars available for purchasing content use) or abstract (e.g. a total number of permitted usages)." (IT Glossary, 3/7/95, IT00709617) 5. Budget: "*A fixed quantity of money, time, etc. against which the cost of operation is charged. Budget activities usually also involve reporting." (IT Glossary, 8/21/95, IT0032371)

[1] "IT Glossary" herein is a generic reference to several "glossaries" that have been created by InterTrust and that are further identified by Bates number and/or IT document number.

	Claim Term/Phrase	Evidence Supporting MS Construction
4.	clearinghouse 193.19	**Intrinsic**: 1. "Distribution involves three types of entity. Creators usually are the source of distribution. They typically set the control structure 'context' and can control the rights which are passed into a distribution network. Distributors are users who form a link between object (content) end users and object (content) creators. They can provide a two-way conduit for rights and audit data. Clearinghouses may provide independent financial services, such as credit and/or billing services, and can serve as distributors and/or creators. Through a permissions and budgeting process, these parties collectively can establish fine control over the type and extent of rights usage and/or auditing activities." ('193 267:34-45) 2. "Payment credit or currency may then be automatically communicated in protected (at least in part encrypted) form through telecommunication of a VDE container to an appropriate party such as a clearinghouse, provider of original property content or appliance, or an agent for such provider (other than a clearinghouse)." ('193 36:64 - 37:3) 3. "...if appropriate credit (e.g. an electronic clearinghouse account from a clearinghouse such as VISA or AT&T) is available..." ('193 25:22-24) **Extrinsic:** 4. Clearinghouse: "*A facility that receives reports of content use and in turn reports payments and usage to content creators and distributors." (IT Glossary, 8/21/95, TD00068B, IT00032372)
5.	compares 900.155	**Intrinsic**: 1. "ROS 602 also provides a tagging and sequencing scheme that may be used within the loadable component assemblies 690 to detect tampering by substitution. Each element comprising a component assembly 690 may be loaded into an SPU 500, decrypted using encrypt/decrypt engine 522, and then tested/compared to ensure that the proper element has been loaded. Several independent comparisons may be used to ensure there has been no unauthorized substitution. For example, the public and private copies of the element ID may be compared to ensure that they are the same, thereby preventing gross substitution of elements." ('193 87:41-51) **Extrinsic:** 1. Compare: "1. To examine two items to discover their relative magnitudes, their relative positions in an order or in a sequence, or whether they are identical in given characteristics. 2. To examine two or more items for identity, similarity, equality, relative magnitude, or order in a sequence." (IBM) 2. Comparison: "The process of examining two or more items for identity, similarity, equality, relative magnitude, or for order in sequence." (IBM)
6.	component assembly 912.8, 912.35	**Intrinsic**: 1. "Many such load modules are inherently configurable, aggregatable, portable, and extensible and singularly, or in combination (along with associated data), run as control methods under the VDE transaction operating environment." ('193 25:48-52)

	Claim Term/Phrase	Evidence Supporting MS Construction
		2. "Much of the functionality provided by ROS 602 in the preferred embodiment may be based on 'components' that can be securely, independently deliverable, replaceable and capable of being modified (e.g., under appropriately secure conditions and authorizations). Moreover, the 'components' may themselves be made of independently deliverable elements. ROS 602 may assemble these elements together (using a construct provided by the preferred embodiment called a 'channel') at execution time. For example, a 'load module' for execution by SPU 500 may reference one or more 'method cores,' method parameters and other associated data structures that ROS 602 may collect and assemble together to perform a task such as billing or metering. Different users may have different combinations of elements, and some of the elements may be customizable by users with appropriate authorization." ('193 77:12-27) 3. "As discussed above, ROS 602 in the preferred embodiment is a component-based architecture. ROS VDE functions 604 may be based on segmented, independently loadable executable 'component assemblies' 690. These component assemblies 690 are independently securely deliverable. The component assemblies 690 provided by the preferred embodiment comprise code and data elements that are themselves independently deliverable. Thus, each component assembly 690 provided by the preferred embodiment is comprised of independently securely deliverable elements which may be communicated using VDE secure communication techniques, between VDE secure subsystems. These component assemblies 690 are the basic functional unit provided by ROS 602. The component assemblies 690 are executed to perform operating system or application tasks. Thus, some component assemblies 690 may be considered to be part of the ROS operating system 602, while other component assemblies may be considered to be 'applications' that run under the support of the operating system." ('193 83:11-22) 4. "A complete VDE process to service a 'use event' may typically be constructed as a combination of methods 1000." ('193 181:20-21) 5. "The audit information may be, in part, or whole, in some summary and/or analyzed form further processed at the clearinghouse and/or may be combined with other information to form a, at least in part, derived set of information and inserted into one or more at least in part secure VDE objects to be communicated to said one or more (further) auditor parties." ('193 272:29-36) 6. "Components 690 are preferably designed to be easily separable and individually loadable. ROS 602 assembles these elements together into an executable component assembly 690 prior to loading and executing the component assembly (e.g., in a secure operating environment such as SPE 503 and/or HPE 655)." ('193 83:43-48) 7. "component assemblies 690" ('193 83:23); see also "components 690" ('193 86:51-52) 8. "In the preferred embodiment, ROS 602 assembles component assemblies 690 based on the following types of elements: Permissions Records ('PERC's) 808; Method 'Cores' 1000; Load Modules 1100; Data Elements (e.g., User Data Elements ('UDEs') 1200 and Method Data Elements ('MDEs') 1202); and Other component assemblies 690." ('193 85:21-29)

	Claim Term/Phrase	Evidence Supporting MS Construction
		9. "…creation of component assemblies 690 from independently deliverable modules such as method cores 1000, load modules 1100, and data structures such as UDEs 1200." ('193 170:2-4) 10. "ROS 602 also provides a tagging and sequencing scheme that may be used within the loadable component assemblies 690 to detect tampering by substitution. Each element comprising a component assembly 690 may be loaded into an SPU 500, decrypted using encrypt/decrypt engine 522, and then tested/compared to ensure that the proper element has been loaded. Several independent comparisons may be used to ensure there has been no unauthorized substitution. For example, the public and private copies of the element ID may be compared to ensure that they are the same, thereby preventing gross substitution of elements. In addition, a validation/correlation tag stored under the encrypted layer of the loadable element may be compared to make sure it matches one or more tags provided by a requesting process. This prevents unauthorized use of information. As a third protection, a device assigned tag (e.g., a sequence number) stored under an encryption layer of a loadable element may be checked to make sure it matches a corresponding tag value expected by SPU 500. This prevents substitution of older elements. Validation/correlation tags are typically passed only in secure wrappers to prevent plaintext exposure of this information outside of SPU 500." ('193 87:41-62) 11. "Memory manager 578 and virtual memory manager 580 in the preferred embodiment manage ROM 532 and RAM 534 memory within SPU 500 in the preferred embodiment. Virtual memory manager 580 provides a fully 'virtual' memory system to increase the amount of 'virtual' RAM available in the SPE secure execution space beyond the amount of physical RAM 534a provided by SPU 500. Memory manager 578 manages the memory in the secure execution space, controlling how it is accessed, allocated and deallocated. SPU MMU 540, if present, supports virtual memory manager 580 and memory manager 578 in the preferred embodiment. In some 'minimal' configurations of SPU 500 there may be no virtual memory capability and all memory management functions will be handled by memory manager 578. Memory management can also be used to help enforce the security provided by SPE 503. In some classes of SPUs 500, for example, the kernel memory manager 578 may use hardware memory management unit (MMU) 540 to provide page level protection within the SPU 500. Such a hardware-based memory management system provides an effective mechanism for protecting VDE component assemblies 690 from compromise by 'rogue' load modules." ('193 109:24-45) 12. "The channel 594 and its header 596 comprise a data structure that 'binds' or references elements of one or more component assemblies 690. Thus, the channel 594 is the mechanism in the preferred embodiment that collects together or assembles the elements shown in FIG. 11E into a component assembly 690 that may be used for event processing." ('193 115:65 - 116:4) 13. "It reads the appropriate open control elements from the secure database (or the container, such as, for example, in the case of a traveling object), and 'binds' or 'links' these particular appropriate control elements together in order to control opening of the object for this user." ('193 185:42-46)

	Claim Term/Phrase	Evidence Supporting MS Construction
		14. "Thus, PERC 808 in effect contains a 'list of assembly instructions' or a 'plan' specifying what elements ROS 602 is to assemble together into a component assembly and how the elements are to be connected together. PERC 808 may itself contain data or other elements that are to become part of the component assembly 690." ('193 85:30-39) 15. "The selected method event record 1012, in turn, specifies the appropriate information (e.g., load module(s) 1100, data element UDE(s) and MDE(s) 1200, 1202, and/or PERC(s) 808) used to construct a component assembly 690 for execution in response to the event that has occurred. ..." ('193 138:31-36) 16. "As mentioned above, ROS 602 provides several layers of security to ensure the security of component assemblies 690. One important security layer involves ensuring that certain component assemblies 690 are formed, loaded and executed only in secure execution space such as provided within an SPU 500. Components 690 and/or elements comprising them may be stored on external media encrypted using local SPU 500 generated and/or distributor provided keys." ('193 87:33-40) 17. "ROS 602 also provides a tagging and sequencing scheme that may be used within the loadable component assemblies 690 to detect tampering by substitution." ('193 87:41-43) 18. "ROS 602 generates component assemblies 690 in a secure manner. As shown graphically in FIGS. 11I and 11J, the different elements comprising a component assembly 690 may be 'interlocking' in the sense that they can only go together in ways that are intended by the VDE participants who created the elements and/or specified the component assemblies. ROS 602 includes security protections that can prevent an unauthorized person from modifying elements, and also prevent an unauthorized person from substituting elements." ('193 84:60 - 85:2) 19. "ROS 602 assembles these elements together into an executable component assembly 690 prior to loading and executing the component assembly (e.g., in a secure operating environment such as SPE 503 and/or HPE 655). ROS 602 provides an element identification and referencing mechanism that includes information necessary to automatically assemble elements into a component assembly 690 in a secure manner prior to, and/or during, execution." ('193 83:44-52) 20. "Wherein said processor includes: retrieving means for retrieving at least one component, and at least one record that specifies a component assembly, from said memory devices, checking means coupled to said retrieving means for checking said component and/or said record for validity, and using means coupled to said retrieving means for using said component to form said component assembly in accordance with said record." ('107 Application p. 782 claim 80) 21. "These called-for method(s) and data structure(s) (e.g., load modules 1100, UDEs 1200 and/or MDEs 1202) are each decrypted using encrypt/decrypt manager 556 (if necessary), and are then each validated using key and tag manager 558. Channel manager 562 constructs any necessary 'jump table' references to, in effect, 'link' or 'bind' the elements into a single cohesive executable so the load module(s) can reference data structures and any other load module(s) in the

	Claim Term/Phrase	Evidence Supporting MS Construction
		component assembly. Channel manager 562 may then issue calls to LMEM 568 to load the executable as an active task." ('193 116:25-35) **Extrinsic:** 1. Component: "1. Hardware or software that is part of a functional unit. 2. A functional part of an operating system. 3. A set of modules that performs a major function within a system." (IBM) 2. Component: "In data communications, a device or set of devices, consisting of hardware, along with its firmware, and or software that performs a specific function on a computer communications network. A Component is a part of a larger system, and may itself consist of other components." (Longley) 3. Record: "1. In programming languages, an aggregate that consists of data objects, possibly with different attributes, that usually have identifiers attached to them. In some programming languages, records are call structures. 2. A set of data treated as a unit. 3. A set of one or more related data items grouped for processing." (IBM) 4. Record: "1. In computing, a collection of related data treated as a unit, e.g. details of name, address, age, occupation and department of an employee in a personnel file. 2. In computing, to store signals on a recording medium for later use." (Longley) 5. Record: "1. A collection of related data or words treated as a unit and saved in a position dependent fashion within a file or other such unit. 2. A set of data items, called fields, treated as a unit." (Booth) 6. Secure: "Pertaining to the control of who can use an object and to the extent to which the object can be used by controlling the authority given to the user." (IBM)
7.	contain 683.2 912.8, 912.35	**Intrinsic:** 1. "Container 300y may contain and/or reference rules and control information 300y(1) that specify the manner in which searching and routing information use and any changes may be paid for." ('193 241:36-39) 2. "Each logical object structure 800 may also include a 'private body' 806 containing or referencing a set of methods 1000 (i.e., programs or procedures) that control use and distribution of the object 300." ('193 128:25-28) 3. "Therefore, stationary object structure 850 does not contain a permissions record (PERC) 808; rather, this permissions record is supplied and/or delivered separately (e.g., at a different time, over a different path, and/or by a different party) to the appliance/installation 600." ('193 130:18-22) 4. "The content portion of a logical object may be organized as information contained in, not contained in, or partially contained in one or more objects." ('193 127:8-19) 5. "Container 302 may 'contain' items without those items actually being stored within the container. For example, the container 302 may reference items that are available elsewhere such as in other containers at remote sites. Container 302 may reference items available at different times or only during limited times. Some items may be too large to store within container 302. Items may, for example, be delivered to the user in the form of a 'live feed' of video at a certain

	Claim Term/Phrase	Evidence Supporting MS Construction
		time. Even then, the container 302 'contains' the live feed (by reference) in this example." ('193 58:49-58) 6. "Load modules 1100 may contain or reference other load modules." ('193 86:47-48) 7. "PERC 808(k) defines, among other things, the 'assembly instructions' for component assembly 690(k), and may contain or reference parts of some or all of the components that are to be assembled to create a component assembly." ('193 87:3-6) 8. "Alternatively, traveling object PERCs 808 may contain or reference budget records..." ('193 130:63-64) 9. "Method 'core' 1000' in the preferred embodiment may contain or reference one or more data elements such as MDEs 1202 and UDEs 1200." ('193 136:32-34) 10. "Container 300y may contain and/or reference rules and control information 300y(1) that specify the manner in which searching and routing information use and any changes may be paid for." ('193 241:36-39) 11. "Trusted go-between 4700 registers the contract 4068, and then creates an electronic list of rules based on contract 4068. A partial example rule list is shown in FIG. 130A. Although the FIG. 130A conditions are shown as being written on a clipboard, in the preferred embodiment the" ('683 54:29-37) 12. See also prior art referred to in the relevant InterTrust patent file histories, e.g. U.S. Patent No. 5,715,403 **Extrinsic:** 1. Container: "contains protected *content*, which is divided into one or more *atomic elements*, and, optionally, *PERCs* governing the *content* and may be manipulated only as specified by a *PERC.*" (IT Glossary, 4/6/95, IT00028206) 2. Container: "A packaging mechanism, consisting of: *One or more Element-derived components. *An organization mechanism which provides a unique name within a flat namespace for each of the components in a Container." (IT Glossary, 5/12/95, IT00028293) 3. Container: "A protected digital information storage and transport mechanism for packaging content and control information." (IT Glossary, 8/21/95, TD00068B, IT00032372) 4. Container: "A collection of content and control-related information." (IT VDE Container Overview, 2/10/95, ETM-9999 Version 0.21, IT00051228) 5. Container: "A dynamic data structure, the elements of which are arbitrary data items whose type is not known when the program is written." (Que) 6. Container: "Abstract data type storing a collection of objects (elements)." (Laplante) 7. See also IT00037-44, IT002734-39, IT004188-96, IT0031572-85, IN00075960, IT00703055-71, IT0052146-64, IN00441189-224, IN0075983-87 8. Contain: "In data security, a multilevel information structure. A container has a classification and may contain objects and/or other containers." (Longley) 9. U.S. Patent No. 5,369,702 10. See also Microsoft PLR 4-2 Exhs. E & F as revised, and InterTrust's Rule 30(b)(6) testimony.

	Claim Term/Phrase	Evidence Supporting MS Construction
8.	control (n.) 193.1, 193.11, 193.15, 193.19 683.2 891.1	**Intrinsic**: 1. "Claims ... are allowable over the prior art of record. The instant claims provide for first and second entity or control or procedure or executable code that are separately, remotely and different from each to combine or process or execute an operation or procedure based on at least first and second control or procedure or executable code in an electronic appliance or secure operating environment or third party different and remote from the first and second entity or control or procedure or executable code." (08/964,333 Patent Application Prosecution History, Office Action, 9/22/98, p. 3 (MSI028945)) 2. "The virtual distribution environment 100 prevents use of protected information except as permitted by the 'rules and controls' (control information)." ('193 56:26-28) 3. "As mentioned above, virtual distribution environment 100 'associates' content with corresponding 'rules and controls,' and prevents the content from being used or accessed unless a set of corresponding 'rules and controls' is available." ('193 57:18-22) 4. "...at least one rule and/or control associated with the software agent that governs the agent's operation." ('193 241:2-3) 5. "In this example control information may include one or more component assemblies that describe the articles within such a container (e.g. one or more event methods referencing map tables and/or algorithms that describe the extent of each article)." ('193 309:5-9) 6. "Even if a consumer has a copy of a video program, she cannot watch or copy the program unless she has 'rules and controls' that authorize use of the program. She can use the program only as permitted by the 'rules and controls.'" ('193 53:60-63) 7. "A control set 914 contains a list of required methods that must be used to exercise a specific right (i.e., process events associated with a right)." ('193 151:14-16) 8. "If necessary, trusted go-between 4700 may obtain and register any methods, rules and/or controls it needs to use or manipulate the object 300 and/or its contents (FIG. 122 block 4778)." ('683, 47:42-45) 9. "These rights govern use of the VDE object 300 by that user or user group. For instance, the user may have an 'access' right, and an 'extraction' right, but not a 'copy' right." ('193 159:23-26) 10. "To provide for this, ROS 602 may include a 'redirector' 684 that allows such 'non-VDE aware' applications 608(b) to access VDE objects 300 and functions 604. Redirector 684, in the preferred embodiment, translates OS calls directed to the 'other OS functions' 606 into calls to the 'VDE functions' 604. As one simple example, redirector 684 may intercept a 'file open' call from application 608(b), determine whether the file to be opened is contained within a VDE container 300, and if it is, generate appropriate VDE function call(s) to file system 687 to open the VDE container (and potentially generate events to HPE 655 and/or SPE 503 to determine the name(s) of file(s) that may be stored in a VDE object 300, establish a control structure associated with a VDE object 300, perform a registration for a VDE object 300, etc.). Without redirector 684 in this example, a

	Claim Term/Phrase	Evidence Supporting MS Construction
		non-VDE aware application such as 608b could access only the part of API 682 that provides an interface to other OS functions 606, and therefore could not access any VDE functions." ('193 82:27-45) 11. "An executing process cannot access memory outside its domain and can only communicate with other processes through services provided by and mediated by privileged kernel/dispatcher software 552 within the SPU 500." ('193 109:53-57) 12. "An electronic appliance 600 may not access an object unless a corresponding PERC 808 is present, and may only use the object and related information as permitted by the control structures contained within the PERC." ('193 118:17-31) 13. "Load modules are not necessarily directly governed by PERCs 808 that control them, nor must they contain any time/date information or expiration dates. The only control consideration in the preferred embodiment is that one or more methods 1000 reference them using a correlation tag (the value of a protected object created by the load module's owner, distributed to authorized parties for inclusion in their methods, and to which access and use is controlled by one or more PERCs 808). If a method core 1000' references a load module 1100 and asserts the proper correlation tag (and the load module satisfies the internal tamper checks for the SPE 503), then that load module can be loaded and executed, or it can be acquired from, shipped to, updated, or deleted by, other systems." (193 139:60 - 140:6) 14. "In the preferred embodiment, SPE RPC manager 550 first references a service request against the RPC service table to determine the location of the service manager that may service the request. The RPC manager 550 then routes the service request to the appropriate service manager for action. Service requests are handled by the service manager within the SPE 503 using the RPC dispatch table to dispatch the request. Once the RPC manager 550 locates the service reference in the RPC dispatch table, the load module that services the request is called and loaded using the load module execution manager 568. The load module execution manager 568 passes control to the requested load module after performing all required context configuration, or if necessary may first issue a request to load it from the external management files 610." ('193 148:55-58) 15. "Although methods 1000 can have virtually unlimited variety and some may even be user-defined, certain basic 'use' type methods are preferably used in the preferred embodiment to control most of the more fundamental object manipulation and other functions provided by VDE 100. For example, the following high level methods would typically be provided for object manipulation: OPEN method, READ method, WRITE method, CLOSE method. An OPEN method is used to control opening a container so its contents may be accessed. A READ method is used to control the access to contents in a container. A WRITE method is used to control the insertion of contents into a container. A CLOSE method is used to close a container that has been opened." ('193 183:12-29) 16. "FIG. 54 is a flowchart of an example of program control steps performed by an ACCESS method 2000. As described above, an ACCESS method may be used to access content embedded in an object 300 so it can be written to, read from, or

	Claim Term/Phrase	Evidence Supporting MS Construction
		otherwise manipulated or processed. In many cases, the ACCESS method may be relatively trivial since the object may, for example, be stored in a local storage that is easily accessible. However, in the general case, an ACCESS method 2000 must go through a more complicated procedure in order to obtain the object. For example, some objects (or parts of objects) may only be available at remote sites or may be provided in the form of a real-time download or feed (e.g., in the case of broadcast transmissions). Even if the object is stored locally to the VDE node, it may be stored as a secure or protected object so that it is not directly accessible to a calling process. ACCESS method 2000 establishes the connections, routings, and security requisites needed to access the object. These steps may be performed transparently to the calling process so that the calling process only needs to issue an access request and the particular ACCESS method corresponding to the object or class of objects handles all of the details and logistics involved in actually accessing the object." ('193 188:59-67) 17. "The READ control method 1652 must determine which key to use to decrypt content if it is going to release decrypted content to the user (block 1758). READ control method 1652 may make this key determination based, in part, upon the PERC 808 for the object (block 1760). READ control method 1652 may then call an ACCESS method to actually obtain the encrypted content to be decrypted (block 1762). The content is then decrypted using the key determined by block 1758 (block 1764)." ('193 192:2-24) 18. See also prior art referred to in the relevant InterTrust patent file histories, e.g., references made at the following bates ranges: MSI026598-602, MSI26626-7, MSI26630-42; MSI028808-11, MSI28846-52, MSI28728-62, MSI28857-58, MSI28944-97, MSI28953-56 19. "C_C may further include, for example: (a) a requirement that distributors ensure that creator C receive $1 per article accessed by users and/or user/distributors, which payment allows a user to access such an article for a period of no more than six months (e.g. using a map-type meter method that is aged once per month, time aged decryption keys, expiration dates associated with relevant permissions records, etc." ('193 309:10-16) 20. "It also employs a software object architecture for VDE content containers that carries protected content and may also carry both freely available information (e.g, summary, table of contents) and secured content control information which ensures the performance of control information." ('193 15:41-46) 21. "Because of the breadth of issues resolved by the present invention, it can provide the emerging 'electronic highway' with a single transaction/distribution control system that can, for a very broad range of commercial and data security models, ensure against unauthorized use of confidential and/or proprietary information and commercial electronic transactions." ('193 17:22-28) 22. "... (as allowed, or not prevented, by senior control information)." ('193 303:67 - 304:1) 23. "For purposes of expedition, applicants are rewriting these dependent claims into independent form, ... In addition, applicants have ... replaced 'necessary in order to gain' with 'allowing' in now-cancelled claim 204 incorporated into formerly dependent claims 209 & 21 1 [issued claim 35] ...." (Prosecution

	Claim Term/Phrase	Evidence Supporting MS Construction
		History for the 08/780,545 Patent Application (issued as the '912), Amendment, 10/29/98) 24. "VDE can: (a) audit and analyze the use of content, (b) ensure that content is used only in authorized ways, and (c) allow information regarding content usage to be used only in ways approved by content users." ('193 4:51-56) 25. "VDE is a secure system for regulating electronic conduct and commerce. Regulation is ensured by control information put in place by one or more parties." ('193 6:33-34) 26. "VDE ensures that certain prerequisites necessary for a given transaction to occur are met." ('193 20:27-28) **Extrinsic:** 1. Control: "The determination of the time and order in which the parts of a data processing system and the devices that contain those parts perform the input, processing, storage, and output functions." (IBM) 2. "5. Control Notes ... A Control must execute as a transaction ... A Control may require pre-conditions – that is that one or more other Controls have been executed before the Control is executed. ... 7. Control Execution Flow The following pseudocode describes the approximate execution sequence for a View Control ... 8. Operation of a Control (Execution of 'Rules and Consequences') ..." (VDE Controls Notes, IT00051953-55) 3. Control: "A business rule that governs the use of content." (IT Glossary, 1997-1998, ML00012B) 4. Control: "A set of rules and consequences that apply to a governed element. The term control can apply to either a control program or a control set." (IT Glossary, 1997-2000, ML00012D) 5. Control: "**Control Element*: A data structure that givems [sic] the operation of a control mechanism (e.g., meter element, budget element, report element, trail element). **Control mechanism*: One of the mechanisms that controls and performs operations on a VDE object (e.g. meter, bill, budget). A control mechanism is distinct from a control element in that it specifies the execution of some process. * *Control object:* A data structure that is used to implement some VDE control: a PERC, a control element, a control parameter, or the data representing a control mechanism. **Control Parameter:* A data structure that is input to a control mechanism and that serves as part of the mechanism's specifications. For example, a billing mechanism might have a pricing parameter; a creator using that mechanism could alter the parameter but not change the mechanism itself." (IT Glossary, 3/7/95, IT00709618) 6. Control: "Defines rules and consequences for operations on a Property Chunk. A Control may be implemented by a process of arbitrary complexity (within the limits posed by the capability of the Node." (IT Glossary, 5/12/95, IT00028293) 7. Control: "A set of rules and consequences for operations on content, such as pricing, payment models, usage reporting etc." (IT Glossary, 8/21/95, TD00068B, IT00032373) 8. Control: "An object of the InterTrust Commerce Architecture that specifies business rules. Controls are applied at any time and at any point in the Chain of

	Claim Term/Phrase	Evidence Supporting MS Construction
		Handling and Control. InterTrust controls are dynamic, independent, and persistent." (IT Glossary, 11/17/96, TD00189J, IT00035865) 9. "'Rules and Controls' means any electronic information that directs, enables, specifies, describes, and/or provides contributing means for performing or not-performing, permitted and/or required operations related to Content, including, for example, restricting or otherwise governing the performance of operations, such as, for example, Management of such Content." (License Agreement, InterTrust/Universal Music Group, 4/13/99, Exhibit 11 to InterTrust 30(b)(6)) 10. "A set of control elements corresponding to all of the property elements of a property. There may be zero or more controls for a given property." (IT 0028204) 11. "CONTROL(S): Controls refer to the rules and consequences associated with DigiBox containers. Controls may be applied dynamically..." (IT00035961) 12. "CONTROL: The rules associated with a governed entity such as a DigiBox container, property, or another control ... applied dynamically. InterTrust controls are dynamic, independent, and persistent." (IT00035920) 13. "... controls implement business rules..." (IT00035892) 14. "The function of performing required operations when certain specific conditions occur or when interpreting and acting upon instructions." (Webster's) 15. Access (n.): "2. The use of an access method. 3. The manner in which files or data sets are referred to by the computer. ... 5. In computer security, a specific type of interaction between a subject and an object that results in the flow of information from one to the other." (IBM) 16. Access (n.): "1. In access control, a specific type of interaction between a subject and an object that results in the flow of information from one to the other ... 3. In computing, the manner in which files or data sets are referred to by a computer." (Longley) 17. Access(ing) (v.): "1. To obtain the use of a computer resource. ... 4. To obtain data from or to put data in storage." (IBM) 18. Least privilege: "Each user and each program should operate using the fewest privileges possible. In this way, the damage from an inadvertent or malicious attack is minimized." (Pfleeger) 19. See also IT00125, IT31410-14, IT703083-89, IT51721-26, IT00735936 (key), IT51956 et seq., IN0075983-87, IN0075989-93 20. See also Microsoft PLR 4-2 Exhs. E & F as revised, and InterTrust's Rule 30(b)(6) testimony.
9.	controlling, control (v.) 193.1 861.58	**Intrinsic:** 1. "ROS 602 includes software intended for execution by SPU microprocessor 520 for, in part, controlling usage of VDE related objects 300 by electronic appliance 600. As will be explained, these SPU programs include 'load modules' for performing basic control functions." ('193 66:5-8) 2. "VDE prevents many forms of unauthorized use of electronic information, by controlling and auditing (and other administration of use) electronically stored and/or disseminated information." ('193 11:60-63) 3. "It also employs a software object architecture for VDE content containers that carries protected content and may also carry both freely available information

	Claim Term/Phrase	Evidence Supporting MS Construction
		(e.g., summary, table of contents) and secured content control information which ensures the performance of control information." ('193 15:41-46) 4. "VDE ensures that certain prerequisites necessary for a given transaction to occur are met." ('193 20:27-28) 5. "The virtual distribution environment 100 prevents use of protected information except as permitted by the 'rules and controls' (control information)." ('193 56:26-28) 6. "As mentioned above, virtual distribution environment 100 'associates' content with corresponding 'rules and controls,' and prevents the content from being used or accessed unless a set of corresponding 'rules and controls' is available." ('193 57:18-22) 7. "VDE can: (a) audit and analyze the use of content, (b) ensure that content is used only in authorized ways, and (c) allow information regarding content usage to be used only in ways approved by content users." ('193 4:51-56) 8. "VDE is a secure system for regulating electronic conduct and commerce. Regulation is ensured by control information put in place by one or more parties." ('193 6:33-35) 9. "It also employs a software object architecture for VDE content containers that carries protected content and may also carry both freely available information (e.g., summary, table of contents) and secured content control information which ensures the performance of control information." ('193 15:41-46) 10. "Because of the breadth of issues resolved by the present invention, it can provide the emerging 'electronic highway' with a single transaction/distribution control system that can, for a very broad range of commercial and data security models, ensure against unauthorized use of confidential and/or proprietary information and commercial electronic transactions." ('193 17:22-28) 11. "VDE ensures that certain prerequisites necessary for a given transaction to occur are met." ('193 20:27-28) **Extrinsic:** 1. Control: "The determination of the time and order in which the parts of a data processing system and the devices that contain those parts perform the input, processing, storage, and output functions." (IBM) 2. Control: "A business rule that governs the use of content." (IT Glossary, 1997-1998, ML00012B) 3. Control: "A set of rules and consequences that apply to a governed element. The term control can apply to either a control program or a control set." (IT Glossary, 1997-2000, ML00012D) 4. Control: "**Control Element*: A data structure that giverns (*sic)* the operation of a control mechanism (e.g., meter element, budget element, report element, trail element). **Control mechanism*: One of the mechanisms that controls and performs operations on a VDE object (e.g. meter, bill, budget). A control mechanism is distinct from a control element in that it specifies the execution of some process. * *Control object:* A data structure that is used to implement some VDE control: a PERC, a control element, a control parameter, or the data representing a control mechanism. **Control Parameter:* A data structure that is

	Claim Term/Phrase	Evidence Supporting MS Construction
		input to a control mechanism and that serves as part of the mechanism's specifications. For example, a billing mechanism might have a pricing parameter; a creator using that mechanism could alter the parameter but not change the mechanism itself." (IT Glossary, 3/7/95, IT00709618) 5. Control: "Defines rules and consequences for operations on a Property Chunk. A Control may be implemented by a process of arbitrary complexity (within the limits posed by the capability of the Node." (IT Glossary, 5/12/95, IT00028293) 6. Control: "A set of rules and consequences for operations on content, such as pricing, payment models, usage reporting etc." (IT Glossary, 8/21/95, TD00068B, IT00032373)
10.	copy, copied, copying 193.1, 193.11, 193.15, 193.19	**Intrinsic**: 1. "These rights govern use of the VDE object 300 by that user or user group. For instance, the user may have an 'access' right, and an 'extraction' right, but not a 'copy' right." ('193 159:23-26) 2. "At the same time, electronic testing will allow users to receive a copy (encrypted or unencrypted) of their test results when they leave the test sessions." ('193 319:12-15) 3. "This is because VDE objects may contain data that can be electronically copied outside the confines of a VDE node. If the content is encrypted, the copies will also be encrypted and the copier cannot gain access to the content unless she has the appropriate decryption key(s)." ('193 129:3-8) 27. "Even if a consumer has a copy of a video program, she cannot watch or copy the program unless she has 'rules and controls' that authorize use of the program. She can use the program only as permitted by the 'rules and controls.'" ('193 53:60-63) 4. "For example, if a software program was distributed as a traveling object, a user of the program who wished to supply it or a usable copy of it to a friend would normally be free to do so." ('193 131:65 - 132:1) 5. "Storing a first digital file and a first control in a first secure container, said first control constituting a first budget which governs the number of copies which may be made of said first digital file or a portion of said first digital file while said first digital file is contained in said first secure container." ('193 330:1 -331:25 (claim 60)) **Extrinsic:** 1. Copy: "A product of a document copying process." (IBM)
11.	derive 900.155	**Intrinsic**: 1. "Such control information can continue to manage usage of container content if the container is 'embedded' into another VDE managed object, such as an object which contains plural embedded VDE containers, each of which contains content derived (extracted) from a different source." ('193 28:60-65)
12.	designating 721.1	

	Claim Term/Phrase	Evidence Supporting MS Construction
13.	device class 721.1	**Intrinsic**: 1. "Furthermore, Applicants respectfully submit that some of the terms cited by the Examiner as 'indefinite' are either well-known by persons skilled in the art or inherently clear. For example, in Claims 1-4, 22-25, the term 'class' is used as part of the phrase 'device class.' Applicants respectfully submit that 'device class' is inherently clear, meaning a group of devices which share at least one attribute." (Prosecution History for the 08/689,754 Patent Application (issued as the '721), Amendment, 4/14/99, p. 14) **Extrinsic:** 1. Device: "1. A mechanical, electrical, or electronic contrivance with a specific purpose." (IBM) 2. Device class: "The generic name for a group of device types." (IBM) 3. Device type: "1. The name for a kind of device sharing the same model number; for example, 2311, 2400, 2400-1. Contrast with device class. 2. The generic name for a group of devices; for example, 5219 for IBM 5219 Printers. Contrast with device class." (IBM)
14.	digital signature, digitally signing 721.1	**Intrinsic:** 1. "There exist many well known processes for creating digital signatures. One example is the Digital Signature Algorithm (DSA). DSA uses a public-key signature scheme that performs a pair of transformations to generate and verify a digital value called a 'signature.'" ('721 10:60-64) 2. "A verifying authority digitally 'signs' and 'certifies' those load modules or other executables it has verified (using a public key based digital signature and/or certificate based thereon, for example)." ('721 4:64-67) 3. "The algorithm also makes use of a one-way hash function, H(m), such as, for example, the Secure Hash Algorithm. The first three parameters, p, q, and g, are public and may be shared across a network of users. The private key is x; the public key is y. To sign a message, m, using DSA, a signer generates a random number, k, less than q. The signer also generates: $r=(g^k \bmod p) \bmod q$; and $s=(k^{-1}(H(m)+xr)) \bmod q$. The parameters r and s comprise the signer's signature, which may be sent to a recipient or distributed across a network." ('721 11:7-22) 4. "Protected processing environment 108 then decrypts digital signature 106 using the second key 124--i.e., it opens strongbox 118 to retrieve the message digest 116 a verifying authority 100 placed in there. Protected processing environment 108 compares the version of message digest 116 it obtains from the digital signature 106 with the version of message digest 116' it calculates itself from load module 54 using the one way hash transformation 115. The message digests 116, 116' should be identical. If they do not match, digital signature 106 is not authentic or load module 54 has been changed--and protected processing environment 108 rejects load module 54." ('721 14:49-60) 5. "One digital signature 106(1) can be created by encrypting message digest 116 with a 'private' key 122(1), another (different) digital signature 106(2) can be created by encrypting the message digest 116 with a different 'private' key 122(2), possibly employing a different signature algorithm." ('721 14:64 - 15:2) 6. "Certificates play an important role in the trustedness of digital signatures, and

	Claim Term/Phrase	Evidence Supporting MS Construction
		also are important in the public-key authentication communications protocol (to be discussed below). In the preferred embodiment, these certificates may include information about the trustedness/level of security of a particular VDE electronic appliance 600 (e.g., whether or not it has a hardware-based SPE 503 or is instead a less trusted software emulation type HPE 655) that can be used to avoid transmitting certain highly secure information to less trusted/secure VDE installations." ('193 203:58-67) 7. "Master Keys: A 'master' key is a key used to encrypt other keys. An initial or 'master' key may be provided within PPE 650 for communicating other keys in a secure way. During initialization of PPE 650, code and shared keys are downloaded to the PPE. Since the code contains secure convolution algorithms and/or coefficients, it is comparable to a 'master key.' The shared keys may also be considered 'master keys.'" ('193 212:12-18) 8. "FIGS. 64 through 67 illustrate the preferred public-key embodiment, but may also be used to help understand the secret-key versions. In secret-key embodiments, the certification process and the public key encryptions/decryptions are replaced with private-key encryptions, and the public key/private-key pairs are replaced with individual secret keys that are shared between the PPE 650 instance and the other parties (e.g., the load module supplier(s), the PPE manufacturer). In addition, the certificate generation process 2804 is not performed in secret-key embodiments, and no site identity certificates 2823 or VDE certificate database 2830 exist." ('193 211:18-30) 9. "Key Types The detailed descriptions of key types below further explain secret-key embodiments; this summary is not intended as a complete description. The preferred embodiment PPE 650 can use different types of keys and/or different 'shared secrets' for different purposes. Some key types apply to a Public-Key/Secret Key implementation, other keys apply to a Secret Key only implementation, and still other key types apply to both. The following table lists examples of various key and 'shared secret' information used in the preferred embodiment, and where this information is used and stored:

Key/Secret Information Type	Used in PK or Non-PK	Example Storage Location(s)
Master Key(s) (may include some of the specific keys mentioned below)	Both	PPE Manufacturing facility VDE administrator
Manufacturing Key	Both (PK optional)	PPE (PK case) Manufacturing facility
Certification key pair	PK	PPE Certification repository
Public/private key pair	PK	PPE Certification repository (Public Key only)
Initial secret key	Non-PK	PPE
PPE manufacturing ID	Non-PK	PPE
Site ID, shared code, shared keys and shared secrets	Both	PPE
Download authorization key	Both	PPE

	Claim Term/Phrase	Evidence Supporting MS Construction
		VDE administrator External communication keys and other info — Both — PPE, Secure Database Administrative object keys — Both — Permission record Stationary object keys — Both — Permission record Traveling object shared keys — Both — Permission record Secure database keys — Both — PPE Private body keys — Both — Secure database, Some objects Content keys — Both — Secure database, Some objects Authorization shared secrets — Both — Permission record Secure Database Back up keys — Both — PPE, Secure database" ('193 211:31 – 212:11) 10. "The process for this selection is similar to the process used by EVENT methods to map events into atomic element numbers. DECRYPT method 2030 may then access an appropriate PERC 808 from the secure database 610 and loads a key (or 'seed') from a PERC (blocks 2034, 2036). This key information may be the actual decryption key to be used to decrypt the content, or it may be information from which the decryption key may be at least in part derived or calculated. If necessary, DECRYPT method 2030 computes the decryption key based on the information read from PERC 808 at block 2034 (block 2038). DECRYPT method 2030 then uses the obtained and/or calculated decryption key to actually decrypt the block of encrypted information (block 2040). DECRYPT method 2030 outputs the decrypted block (or the pointer indicating where it may be found), and terminates (termination point 2042)." ('193 193:8-23) 11. "A 'time aged key' in the preferred embodiment is not a 'true key' that can be used for encryption/decryption, but rather is a piece of information that a PPE 650, in conjunction with other information, can use to generate a 'true key.' This other information can be time-based, based on the particular 'ID' of the PPE 650, or both. Because the 'true key' is never exposed but is always generated within a secure PPE 650 environment, and because secure PPEs are required to generate the 'true key,' VDE 100 can use 'time aged' keys to significantly enhance security and flexibility of the system." ('193 207:50-60) 12. "Running the function with a time-aged key and inappropriate time values typically yields a useless key that will not decrypt." ('193 208:38-40) **Extrinsic:** 1. Digital Signature: "In computer security, encrypted data, appended to or part of a message, that enables a recipient to prove the identity of the sender." (IBM) 2. Digital Signature: "1. In authentication, data appended to, or a cryptographic transformation of, a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery. 2. In authentication, a data block appended to a message, or a complete encrypted message, such that the recipient can authenticate the message contents and/or prove that it could only have originated with the purported sender." (Longley)

	Claim Term/Phrase	Evidence Supporting MS Construction
		3. "Let B be the recipient of a message M signed by A, then A' s [digital] signature must satisfy three requirements: B must be able to validate A's signature on M. It must be impossible for anyone, including B, to forge A's signature. In case A should disavow signing a message M, it must be possible for a judge or third party to resolve a dispute arising between A and B. A digital signature therefore establishes sender authenticity ... it also establishes data authenticity." (Denning, p. 14) 4. "A cipher is unconditionally secure if, no matter how much ciphertext is intercepted, there is not enough information in the ciphertext to determine the plaintext uniquely." (Denning, p. 5) (Davies, pp. 41, 380) 5. "A cipher is computationally secure, or strong, if it cannot be broken by systematic analysis with available resources." (Denning, p. 5) (Davies, pp. 41, 370) 6. Key: "7. In computer security, a sequence of symbols used with a cryptographic algorithm for encrypting or decrypting data." (IBM) 7. Key: "1. In cryptography, a sequence of symbols that controls the operations of encipherment and decipherment. 2. In cryptography, a symbol or sequence of symbols (or electrical or mechanical correlates of symbols) that control the operations of encryption and decryption)." (Longley)
15.	executable programming, executable 721.34 912.8, 912.35	**Intrinsic:** 1. "Furthermore, applicants' independent claims 16, 36, 37 and 64 require secure delivery and use of plural executable items. See claim 16 ('securely delivering a first procedure ... securely delivering ... a second procedure separable or separate from said first procedure...'); claim 36 ('securely delivering plural executable procedures ...'), claim 37 ('securely delivering a first piece of executable code ... securely delivering a second piece of executable code ...') and claim 64 ('securely receiving a first load module ... securely receiving a second load module ...'). These features are not taught or suggested by either Rosen or Johnson. Johnson's databases comprise data, not executable code." (Prosecution for the 08/388,107, Patent Application, Amendment, 6/20/97, pp. 24-25) (MSI028848-49) 2. "In addition, Applicants would like to draw the Examiner's attention to other sections of the specification in support of words or phrases cited by the Examiner as 'indefinite.' ... The noun 'executable,' as used in Claims ... 34-36 ..., is defined in the specification on page 7." (Prosecution History for the 08/689,754 Patent Application (issued as the '721 patent), Amendment, 4/14/99, pp. 13-14) (p. 7 of the original specification is '721 2:62 - 3:13 of the issued patent) **Extrinsic:** 1. Execute: "1. To perform the actions specified by a program or a portion of a program." (IBM) 2. Executable Program: "1. A program that has been link-edited and therefore can be run in a processor. 2. The set of machine language instructions that constitute the output from the compilation of a source program." (IBM)

	Claim Term/Phrase	Evidence Supporting MS Construction
16.	host processing environment 900.155	**Intrinsic:** 1. "Portions of ROS 602 in particular may desirably be included in ROM 658 (e.g., 'bootstrap' routines, POST routines, etc. for use in establishing an operating environment for electronic appliance 600 when power is applied)." ('193 63:13-17) 2. "In the preferred embodiment, HPE 655 is a secure processing environment supported by a processor other than an SPU, such as for example an electronic appliance CPU 654 general-purpose microprocessor or other processing system or device. In the preferred embodiment, HPE 655 may be considered to 'emulate' an SPU 500 in the sense that it may use software to provide some or all of the processing resources provided in hardware and/or firmware by an SPU." ('193 79:60-67) 3. "However, in applications where lesser security can be tolerated and/or the cost of an SPU 500 cannot be tolerated, the SPE 503 may be omitted and all secure processing may instead be performed by one or more secure HPEs 655 executing on general- purpose CPUs 654." ('193 81:4-8) 4. "Integrity of Software-Based PPE Security: As discussed above in connection with FIG. 10, some applications may use a software-based protected processing environment 650 (such as a 'host event processing environment' (HPE) 655) providing a software-based tamper resistant barrier 674." ('900 230:57-61) 5. "In one example, the software distribution medium 3370 might include installation materials 3470 and operational materials 3472. The installation materials 3470 may be executed by computer 3372 to install the operational materials 3472 onto the computer's hard disk 3376. The computer 3372 may then execute the operational materials 3472 from its hard disk 3376 to provide software-based protected processing environment 650 and associated software-based tamper resistant barrier 672." ('900 231:23-31) 6. "The operational materials 3472 may provide executable code and associated data structures for providing protected processing environment 650 and associated software-based tamper resistant barrier 674." ('900 236:50-53) 7. "HPE(s) 655 and SPE(s) 503 are self-contained computing and processing environments that may include their own operating system kernel 688 including code and data processing resources." ('193 79:36-39) 8. "HPEs 655 may be provided in two types: secure and not secure." ('193 80:8-9) 9. "[T]his example also includes one or more Host Event Processing Environments ('HPEs') 655 and/or one or more Secure Event Processing Environment ('SPEs') 503 (these environments may be generically referred to as 'Protected Processing Environments' 650)." ('193 79:31-35) 10. "HPEs 655 may (as shown in FIG. 10) be provided with a software- based tamper resistant barrier 674 that makes them more secure. Such a software-based tamper resistant barrier 674 may be created by software executing on general-purpose CPU 654. Such a 'secure' HPE 655 can be used by ROS 602 to execute processes that, while still needing security, may not require the degree of security provided by SPU 500. This can be especially beneficial in architectures providing both an SPE 503 and an HPE 655. The SPU 502 may be used to perform all truly secure processing, whereas one or more HPEs 655 may be used to provide additional

	Claim Term/Phrase	Evidence Supporting MS Construction
		secure (albeit possibly less secure than the SPE) processing using host processor or other general purpose resources that may be available within an electronic appliance 600. Any service may be provided by such a secure HPE 655" ('193 80:22-36) 11. "The software-based tamper resistant barrier 674 provided by HPE 655 may be provided, for example, by: introducing time checks and/or code modifications to complicate the process of stepping through code comprising a portion of kernel 688a and/or a portion of component assemblies 690 using a debugger; using a map of defects on a storage device (e.g., a hard disk, memory card, etc.) to form internal test values to impede moving and/or copying HPE 655 to other electronic appliances 600; using kernel code that contains false branches and other complications in flow of control to disguise internal processes to some degree from disassembly or other efforts to discover details of processes; using 'self-generating' code (based on the output of a co-sine transform, for example) such that detailed and/or complete instruction sequences are not stored explicitly on storage devices and/or in active memory but rather are generated as needed; using code that 'shuffles' memory locations used for data values based on operational parameters to complicate efforts to manipulate such values; using any software and/or hardware memory management resources of electronic appliance 600 to 'protect' the operation of HPE 655 from other processes, functions, etc. Although such a software-based tamper resistant barrier 674 may provide a fair degree of security, it typically will not be as secure as the hardware-based tamper resistant barrier 502 provided (at least in part) by SPU 500." ('193 80:40-65; Fig. 10) 12. "FIG. 12 also shows that ROS 602 may provide one or more SPEs 503 and/or one or more HPEs 655. As discussed above, HPE 655 may 'emulate' an SPU 500 device, and such HPEs 655 may be integrated in lieu of (or in addition to) physical SPUs 500 for systems that need higher throughput. Some security may be lost since HPEs 655 are typically protected by operating system security and may not provide truly secure processing Thus, in the preferred embodiment, for high security applications at least, all secure processing should take place within SPE 503 having an execution space within a physical SPU 500 rather than a HPE 655 using software operating elsewhere in electronic appliance 600." ('193 88:31-43) 13. "As discussed above in connection with FIG. 12, each electronic appliance 600 in the preferred embodiment includes one or more SPEs 503 and/or one or more HPEs 655. These secure processing environments each provide a protected execution space for performing tasks in a secure manner." ('193 104:39-44) **Extrinsic:** 1. Host processor: "1. A processor that controls all or part of a user application network. 2. In a network, the processing unit in which resides the access method for the network. … 4. A processing unit that executes the access method for attached communication controllers." (IBM) 2. "Host Processing Environment (HPE): A software-only realization of the PPE, protected from tampering by appropriate software techniques. No longer preferred because of the potential confusion between the 'H' in the acronym and

	Claim Term/Phrase	Evidence Supporting MS Construction
		'H' as in 'Hardware' (which this isn't). [REPLACEMENT UNCERTAIN]" (IT Glossary, "Obsolete Terminology Section,"[2] 3/7/95, IT00709621) 3. "Secure Processing Environment (SPE): A hardware-supported realization of the PPE, protected from tampering by physical security techniques. No longer preferred because of the potential confusion between the 'S' in the acronym and 'S' as in 'Software' (which this isn't). [REPLACEMENT UNCERTAIN]" (IT Glossary, "Obsolete Terminology Section" 5/12/95, IT00028302) 4. Environment: See InterTrust node: "A computer that is enabled for processing of DigiBox containers by installation of a PPE, which may be either hardware or software based. A node may include application software and/or operating system integration. The node is also termed the *environment*." (IT Glossary, 8/21/95, TD00068B, IT00032375)
17.	identifier 193.15 912.8	**Intrinsic:** 1. "Portable appliance 2600 RAM 534 may contain, for example, information which can be used to uniquely identify each instance of the portable appliance. This information may be employed (e.g. as at least a portion of key or password information) in authentication, verification, decryption, and/or encryption processes." ('193 230:22-27) 2. "Provide very flexible and extensible user identification according to individuals, installations, by groups such as classes, and by function and hierarchical identification employing a hierarchy of levels of client identification (for example, client organization ID, client department ID, client network ID, client project ID, and client employee ID, or any appropriate subset of the above)." ('193 25:31-38) 3. "Fingerprinting is useful in providing an ability to identify who extracted information in clear form *[sic]* a VDE container, or who made a copy of a VDE object or a portion of its contents." ('193 37:27-31) 4. "All load modules 1100 for use by SPE 503 are preferably referenced by a load module execution manager 568 that maintains and scans a list of available load modules and selects the appropriate load module for execution. If the load module is not present within SPE 503, the task is 'slept' and LMEM 568 may request that the load module 1100 be loaded from secondary storage 562. This request may be in the form of an RPC call to secure database manager 566 to retrieve the load module and associated data structures, and a call to encrypt/decrypt manager 556 to decrypt the load module before storing it in memory allocated by memory manager 578." ('193 111:47-58) 5. "In somewhat more detail, the preferred embodiment executes a load module 1100 by passing the load module execution manager 568 the name (e.g., VDE ID) of the desired load module 1100. LMEM 568 first searches the list of 'in memory' and 'built-in' load modules 572. If it cannot find the desired load

[2] Some terms were "defined" in an "Obsolete Terminology Section" of certain IT Glossaries. This section was described in such documents as: "This section identifies terms that have been used in earlier documents to describe various VDE concepts, but that are, for various reasons, no longer preferred." (See, e.g., IT00028302)

	Claim Term/Phrase	Evidence Supporting MS Construction
		module 1100 in the list, it requests a copy from the secure database 610 by issuing an RPC request that may be handled by ROS secure database manager 744 shown in FIG. 12." ('193 111:59-67) 6. "For each VDE item loaded into SPE 503, Secure Database manager 566 in the preferred embodiment may search a master list for the VDE item ID, and then check the corresponding transaction tag against the one in the item to ensure that the item provided is the current item. Secure Database Manager 566 may maintain list of VDE item ID and transaction tags in a 'hash structure' that can be paged into SPE 503 to quickly locate the appropriate VDE item ID. In smaller systems, a look up table approach may be used. In either case, the list should be structured as a pagable *[sic]* structure that allows VDE item ID to be located quickly." ('193 124:8-18) 7. "A stipulation that the traveling object may be used on certain one or more installations or installation classes or users or user classes where classes correspond to a specific subset of installations or users who are represented by a predefined class identifiers stored in a secure database 610." ('193 131:40-45) 8. "A load module 1100 is able to perform its function only when executed in the protected environment of an SPE 503 or an HPE 655 because only then can it gain access to the protected elements (e.g., UDEs 1200, other load modules 1100) on which it operates. Initiation of load module execution in this environment is strictly controlled by a combination of access tags, validation tags, encryption keys, digital signatures and/or correlation tags. Thus, a load module 1100 may only be referenced if the caller knows its ID and asserts the shared secret correlation tag specific to that load module. The decrypting SPU may match the identification token and local access tag of a load module after decryption. These techniques make the physical replacement of any load module 1100 detectable at the next physical access of the load module." ('193 139:41-55) 9. "These shared secrets may be used during communications processes to permit PPEs 650 to authenticate the identity of other PPEs and/or users." ('193 214:39-41) 10. "As another example, interpreter 508 may provide application 506 with an element identification (e.g., a hexadecimal value or other identifier) that corresponds to the headline information within the newspaper style content (block 558). Application 506 may then ask electronic appliance 500 to provide it with the Headline (or other) content information 102 within container 100 by providing appropriate content information to electronic appliance 500 via APL 504 (block 560)." ('861 12:63 - 13:4) 11. "It is preferable that an extremely secure encryption/decryption technique be used as an aspect of authenticating the identity of electronic appliances 600 that are establishing a communication channel and securing any transferred permission, method, and administrative information." ('193 67:21-26) 12. "As part of the initialization process, the PPE 650 may generate internally or the manufacturer may generate and supply, one or more pairs of site-specific public keys 2815 and private keys 2816. These are used by the PPE 650 to prove its identity." ('193 209:63-67)

	Claim Term/Phrase	Evidence Supporting MS Construction
		Extrinsic: 1. Identifier: "1. One or more characters used to identify or name a data element and possibly to indicate certain properties of that data element. 2. In programming languages, a token that names a data object such as a variable, an array, a record, a subprogram or a function." (IBM) 2. Identifier: "1. In computing, a character or group of characters used to identify, indicate or name a body of data. 2. In computing, a name or string of characters employed to identify a variable, procedure, data structure or some other element of a program." (Longley)
18.	protected processing environment 683.2 721.34	See also "secure" **Intrinsic:** 1. Prosecution History of Application 08/778,256 (continuation of '891 Patent, issued as U.S. Patent No. 5,949,876), Amendment, 1/20/98, pp. 58-60: a. "Independent claims 65 and 76 each recite a 'protected processing environment.' ... Griffeth et al. [U.S. Pat. No. 5,505,837], Yamamoto [U.S. Pat. No. 5,508,913] and Wyman [U.S. Pat. No. 5,260,999] do not disclose these aspects of these claims. b. The system disclosed in Griffeth et al is designed to allow negotiation to proceed in an environment in which a negotiating party does not disclose information about its negotiation goals to the other negotiating party. ... Griffeth et al. does not disclose any privacy protection mechanism and neither teaches nor suggests any secure processing environment or that any operations (e.g., integration or execution) occur securely. Indeed, Griffeth contains no suggestion that any protection mechanism is needed to maintain negotiation goals in privacy, since Griffeth does not suggest that the other party may try to improperly discover information which is intended to remain private. c. Yamamoto states the following: 'Here, the data is enciphered by the data encipher apparatuses 26 so as to maintain confidentiality.' Col. 3, lines 46-47. Since Yamamoto makes no other reference to the encipherment, or to the apparatuses 26, it is impossible to determine how the data encipherment is used, or the roles it plays in the disclosed apparatus. From an examination of Fig. 3, however, it appears that the data encipher apparatuses 26 are placed on connections between a particular site and other, physically separated sites. For example, customer office 23b is connected to sub-center 22 by a line, which apparently represents a communication path. That line connects directly to a data encipher apparatus 26 in customer office 23b, and to another data encipher apparatus 26 in sub-center 22. d. Thus, it appears that the data encipher apparatuses 26 are used, in some undisclosed manner, to encipher at least some data which travels among physically separated locations. It is possible to imagine, for example, that data is enciphered prior to being sent out on an insecure public transmission line, and is then deciphered once received in a new location. e. Yamamoto does not disclose, however, that the processing environments are themselves secure, or that either execution or integration occur in a secure manner or in a secure environment. Indeed, Yamamoto contains no suggestion that security within a processing environment would even be desirable. By

	Claim Term/Phrase	Evidence Supporting MS Construction
		suggesting that data is deciphered once it enters an office (e.g., office 23b), in fact, Yamamoto teaches away from a secure environment, since it would appear that the data is used 'in the clear' within the office, with no suggested protection beyond a simple password for the computer. f. Wyman is equally deficient regarding these elements. Although Wyman specifies that a license may contain a digital signature, therefore rendering the license unforgeable (Col. 14, lines 24-54), Wyman neither teaches nor suggests that the processing environment is itself secure or that any operations occur in a secure manner. The Wyman digital signatures no more suggest a secure processing environment than the requirement that paper contracts be signed in ink suggests that the contracts will be created, read or negotiated in a secure location." 2. "The role of go-between 4700 may, in some circumstances, be played by one of the participant's SPU's 500 (PPEs), since SPU (PPE) behavior is not under the user's control, but rather can be under the control of rules and controls provided by one or more other parties other than the user (although in many instances the user can contribute his or her own controls to operate in combination with controls contributed by other parties)." ('683 24:26-33) 3. "SPU 500 provides a tamper-resistant protected processing environment ("PPE") in which processes and transactions can take place securely and in a trusted fashion." ('683 16:60-62) 4. "The computer 3372 may then execute the operational materials 3472 from its hard disk 3376 to provide software-based protected processing environment 650 and associated software-based tamper resistant barrier 672)." ('900 231:27-31) 5. "The special purpose secure circuitry provided by the present invention includes at least one of: a dedicated semiconductor arrangement known as a Secure Processing Unit (SPU) and/or a standard microprocessor, microcontroller, and/or other processing logic that accommodates the requirements of the present invention and functions as an SPU." ('193 20:58-63) 6. "This means that a VDE SPU can employ (share) circuitry elements of a 'standard' CPU. For example, if a 'standard' processor can operate in protected mode and can execute VDE related instructions as a protected activity, then such an embodiment may provide sufficient hardware security for a variety of applications and the expense of a special purpose processor might be avoided." ('193 21:11-17) 7. "Different protected processing environments (secure execution spaces) might examine different subsets of the multiple digital signatures--so that compromising one protected processing environment (secure execution space) will not compromise all of them." ('721 7:19-23) 8. "The assurance level III appliance 61C shown is a general purpose personal computer equipped with a hardware-based secure processing unit 132 providing and completely containing protected processing environment 108 (see Ginter et al. FIGS. 6 and 9 for example). A silicon-based special purpose integrated circuit security chip is relatively more tamper-resistant than implementations relying on software techniques for some or all of their tamper-resistance." ('721 16:64 - 17:5)

	Claim Term/Phrase	Evidence Supporting MS Construction
		9. "FIG. 10 is a block diagram of one example of a software structure/architecture for Rights Operating System ('ROS') 602 provided by the preferred embodiment. In this example, ROS 602 includes an operating system ('OS') 'core' 679, a user Application Program Interface ('API') 682, a 'redirector' 684, an 'intercept' 692, a User Notification/Exception Interface 686, and a file system 687. ROS 602 in this example also includes one or more Host Event Processing Environments ('HPEs') 655 and/or one or more Secure Event Processing Environments ('SPEs') 503 (these environments may be generically referred to as 'Protected Processing Environments' 650). HPE(s) 655 and SPE(s) 503 are self-contained computing and processing environments that may include their own operating system kernel 688 including code and data processing resources." ('193 79:36-39) 10. "A given electronic appliance 600 may include any number of SPE(s) 503 and/or any number of HPE(s) 655. HPE(s) 655 and SPE(s) 503 may process information in a secure way, and provide secure processing support for ROS 602. For example, they may each perform secure processing based on one or more VDE component assemblies 690, and they may each offer secure processing services to OS kernel 680. In the preferred embodiment, SPE 503 is a secure processing environment provided at least in part by an SPU 500. Thus, SPU 500 provides the hardware tamper-resistant barrier 503 surrounding SPE 503. SPE 503 provided by the preferred embodiment is preferably: small and compact[,] loadable into resource constrained environments such as for example minimally configured SPUs 500[,] dynamically updatable[,] extensible by authorized users[,] integratable into object or procedural environments[, and] secure." ('193 79:39-59) 11. "As shown in FIG. 13, SPE 503 (PPE 650) includes the following service managers/major functional blocks in the preferred embodiment: Kernel/Dispatcher 552 Channel Services Manager 562 SPE RPC Manager 550 Time Base Manager 554 Encryption/Decryption Manager 556 Key and Tag Manager 558 Summary Services Manager 560 Authentication Manager/Service Communications Manager 564 Random Value Generator 565 Secure Database Manager 566 Other Services 592. Each of the major functional blocks of PPE 650 is discussed in detail below." ('193 105:23-41) 12. "I. SPE Kernel/Dispatcher: 552The Kernel/Dispatcher 552 provides an operating system 'kernel' that runs on and manages the hardware resources of SPU 500. This operating system 'kernel' 552 provides a self-contained operating system for SPU 500; it is also a part of overall ROS 602 (which may include multiple OS kernels, including one for each SPE and HPE ROS is controlling/managing). Kernel/dispatcher 552 provides SPU task and memory management, supports

	Claim Term/Phrase	Evidence Supporting MS Construction
		internal SPU hardware interrupts, provides certain 'low level services,' manages 'DTD' data structures, and manages the SPU bus interface unit 530. Kernel/dispatcher 552 also includes a load module execution manager 568 that can load programs into secure execution space for execution by SPU 500." ('193 105:43-57) (see also Fig. 13) 13. "In addition, memory management provided by memory manager 578 operating at least in part based on hardware-based MMU 540 may securely implement and enforce a memory architecture providing multiple protection domains. In such an architecture, memory is divided into a plurality of domains that are largely isolated from each other and share only specific memory areas under the control of the memory manager 578. An executing process cannot access memory outside its domain and can only communicate with other processes through services provided by and mediated by privileged kernel/dispatcher software 552 within the SPU 500. Such an architecture is more secure if it is enforced at least in part by hardware within MMU 540 that cannot be modified by any software-based process executing within SPU 500." ('193 109:46-60) 14. "Secure VDE hardware (also know as SPUs for Secure Processing Units), or VDE installations that use software to substitute for, or complement, said hardware (provided by Host Processing Environments (HPEs)), operate in conjunction with secure communications, system integration software, and distributed software control information and support structures, to achieve the electronic contract/rights protection environment of the present invention. Together, these VDE components comprise a secure, virtual, distributed content and/or appliance control, auditing (and other administration), reporting, and payment environment. In some embodiments and where commercially acceptable, certain VDE participants, such as clearinghouses that normally maintain sufficiently physically secure non-VDE processing environments, may be allowed to employ HPEs rather VDE hardware elements and interoperate, for example, with VDE end-users and content providers." ('193 13:7-23) 15. "Each PPE 650 needs to be initialized before it can be used. Initialization may occur at the manufacture site, after the PPE 650 has been placed out in the field, or both. The manufacturing process for PPE 650 typically involves embedding within the PPE sufficient software that will allow the device to be more completely initialized at a later time. This manufacturing process may include, for example, testing the bootstrap loader and challenge-response software permanently stored within PPE 650, and loading the PPE's unique ID. These steps provide a basic VDE-capable PPE 650 that may be further initialized (e.g., after it has been installed within an electronic appliance 600 and placed in the field). In some cases, the manufacturing and further initialization process may be combined to produce 'VDE ready' PPEs 650." ('193 223:30-44) 16. "In one example, a person with a laptop 5102 or other computer lacking a PPE 650 wishes nonetheless to take advantage of a subset of secure item delivery services." ('683 62:17-20) 17. "Claims 7-11, ... 99-111 ... are rejected under 35 U.S.C. 103(a) as being unpatentable over Fischer (5,412,717) in view of Narasimhalu et al (5,499,298). Fischer discloses a method and apparatus including a system monitor which

	Claim Term/Phrase	Evidence Supporting MS Construction
		limits the ability of a program about to be executed to the use of predefined resources, ... The set of authorities and restrictions are referred to as 'program authorization information' or 'PAI'. ... A comparison of independent claim 7 to Fischer to derive the similarities and differences between the claimed invention and the prior art follows. ... memory containing a first rule corresponds to a first PAI under a first PCB... Here, Fischer provides a secure container in the form of a program, i.e. a governed item, having an associated PAI, i.e. at least one rule associated with the secure container. A protected processing environment ('PPE') protecting at least some information contained in the PPE, see Fischer Terminal A, and including hardware and/or software used for applying said first rule and the secure container in combination to at least in part govern at least one aspect of access to or use of the governed item, see Fischer at Figure 5 and column 10, lines 8-39 where the first rule in memory is first PCB providing a first PAI and the secure container is a program associated with a second PCB providing a first PAI and the secure container is a program associated with a second PCB having a second PAI associated with the governed item, i.e. the program. ... The difference between claim 7 and Fischer is that the PPE disclosed in Fischer is not explicitly disclosed as protected from tampering by a user of the first apparatus, i.e. terminal A. The Narasimhalu patent ... teaches a method and apparatus for controlling the dissemination of digital information [and] that the end user accesses the digital information with a tamper-proof controlled information access device." (Prosecution History for the 09/221,479 Patent Application, (issued as the '683), Office Action, 11/12/99, pp. 3-5 (IT00065799-801)) 18. "With respect to the remaining issues, Applicants respectfully disagree. For example, the Examiner objects to the use of 'environment' as indefinite and unclear. This word, however, is not used in isolation, but rather in the context of several longer phrases, all of which are defined in the specification. The phrase 'protected processing environment,' for example, is used in Claims 11 and 15-18 and described on at least, for example, pages 7-8 and 25 of the specification. The term 'virtual distribution environment' used in Claim 11 is described, for example, on page 7 of the specification. The terms are also described in the commonly copending application Serial Number 08/388,107 of Ginter et al., filed 13 February 1995, entitled 'System and Methods for Secure Transaction Management and Electronic Rights Protection.' A copy of the incorporated Ginter application can be provided to the Examiner upon request." (Prosecution History for the 08/689,754 Patent Application (issued as the '721), Amendment, 4/14/99, p. 13) (pp. 7, 7-8 and 25 of the original specification are '721 2:62 - 3:13, 2:62 - 3:34 and 8:6-28 of the issued patent) 19. "Another approach to supporting COTS software would use the VDE software running on the user's electronic appliance to create one or more 'virtual machine' environments in which COTS operating system and application programs may run, but from which no information may be permanently stored or otherwise transmitted except under control of VDE." ('193 279:26-40) 20. "VDE may be combined with, or integrated into, many separate computers and/or other electronic appliances. These appliances typically include a secure

	Claim Term/Phrase	Evidence Supporting MS Construction
		subsystem that can enable control of content use such as displaying, encrypting, decrypting, printing, copying, saving, extracting, embedding, distributing, auditing usage, etc. The secure subsystem in the preferred embodiment comprises one or more 'protected processing environments'…." ('193 9:22-29) 21. "The operating system 602 may also support at least one 'application' 608. Generally, 'application' 608 is hardware and/or software specific to the context of appliance 600. For example, if appliance 600 is a personal computer, then 'application' 608 could be a program loaded by the user, for instance, a word processor, a communications system or a sound recorder. If appliance 600 is a television controller box, then application 608 might be hardware or software that allows a user to order videos on demand and perform other functions such as fast forward and rewind. In this example, operating system 602 provides a standardized, well defined, generalized 'interface' that could support and work with many different 'applications' 608." ('193 60:51-64) **Extrinsic:** 1. Processing: "1. The performance of logical operations and calculations on data, including temporary retention of data in processor storage while the data is being operated on." (IBM) 2. Environment: "1. The aggregate of external circumstances, conditions, and objects that affect the development, operation, and maintenance of a system. 2. In computer security, those factors, both internal and external, of an ADP system that help to define the risks associated with its operation." (Longley) 3. "The InterTrust architecture employs three principal components: … The InterRights Point software provides 'Protected Processing Environment™' technology for manipulating information in DigiBox containers and for securely implementing business rules." (Panel: The InterTrust Commerce Architecture, D. Van Wie et al., 20th NISSC, p. 2, 1997) 4. Environment: See InterTrust node: "A computer that is enabled for processing of DigiBox containers by installation of a PPE, which may be either hardware or software based. A node may include application software and/or operating system integration. The node is also termed the *environment*." (IT Glossary, 8/21/95, TD00068B, IT00032375) 5. Protected Processing Environment (PPE) technology: "The InterTrust technology that provides the protected software environment within the InterRights Point. Protected Processing Environment technology is responsible for the encryption/decryption of data, protected processing of DigiBox containers, and other secure operations, such as protected database access." (IT Glossary, 1997-1998, ML00012B) 6. Protected Processing Environment (PPE): "The PPE is the secure part of a VDE node: either a hardware or software-protected environment in which VDE mechanisms run without external interference. There are various PPE realizations (e.g., physically protected hardware) appropriate to different operational requirements" (IT Glossary, 3/7/95, IT00709619) 7. Secure Processing Unit: "The physically secure hardware component of the SPE: a processor with local memory and non-volatile storage. The SPE consists of the

	Claim Term/Phrase	Evidence Supporting MS Construction
		SPU itself and the SPE software running on the SPU." (IT Glossary, 3/7/95, IT00709620) 8. Protected Processing Environment (PPE): "An InterTrust *node* has a unique *node ID* and contains a *Protected Processing Environment (PPE)* which performs *operations* on *containers* and *control structures* under rules specified by *PERCs* and which may be realized in a tamper resistant hardware component or in tamper-resistant software and a *protected database*, which stores *control objects* and *InterTrust applications*, operating outside the *PPE*, which manipulate *content* and *control objects* through requests to the *PPE*" (IT Glossary, 4/6/95, IT00028206) 9. "All the terms in italics have specific definitions (in the glossary) with respect to InterTrust." 10. "*Global replace of 'VDE' with 'InterTrust' to match new terminology.*" (IT Glossary, 4/6/95, IT00028206) 11. Protected Environment: "A portion of the node software that uses, and protects, the protected node data such as cryptographic keys. The protected environment is responsible for performing all the protected functions for manipulating containers and content; that is, all the operations governed by controls." (IT Glossary, 5/12/95, IT00028294) 12. Protected Processing Environment: (alternate definition): "The protected environment in which the cryptographic and control functions of InterTrust run. The PPE may be protected environmentally (e.g., as a physically protected server machine) or may employ software-based tamper resistance techniques." (IT Glossary, 8/21/95, TD00068B, IT00032377) 13. Secure Processing Environment (SPE): "A hardware-supported realization of the PPE, protected from tampering by physical security techniques. No longer preferred because of the potential confusion between the 'S' in the acronym and 'S' as in 'Software' (which this isn't).. [REPLACEMENT UNCERTAIN]" (IT Glossary, "Obsolete Terminology Section," 5/12/95, IT00028302) 14. Protected Processing Environment (PPE): "The InterTrust protected software environment within the InterTrust Commerce Node. The PPE is responsible for the encryption/decryption of data, protected processing of DigiBox containers, and other secure operations, such as database access." (IT Glossary, 11/17/96, TD00189J, IT00035871) 15. Process: "(1) in computing, the active system entity through which programs run. The entity in a computer system to which authorizations are granted; thus the unit of accountability in a computer system. (2). In computing, a program in execution. ... (4) In computing, a program is a static piece of code and a process is the execution of that code." (Longley)
19.	secure, securely 193.1, 193.11, 193.15 683.2 721.34	**Intrinsic:** Because this term is indefinite and used inconsistently, each use of "secure" and forms thereof in the asserted patents is relevant and herein included by reference. The following examples are illustrative. 1. "HPEs 655 may be provided in two types: secure and not secure." ('193 80:8-9) 2. "Because secondary storage 652 is not secure, SPE 503 must encrypt and cryptographically seal (e.g., using a one-way hash function initialized with a

	Claim Term/Phrase	Evidence Supporting MS Construction
	861.58 891.1 912.8, 912.35	secret value known only inside the SPU 500) each swap block before it writes it to secondary storage." ('193 107:39-42) 3. "Insecure external memory may reduce the wait time for swapped pages to be loaded into SPU 500, but will still incur substantial encryption/decryption penalty for each page." ('193 125:56-59) 4. "The following is a non-exhaustive list of some of the advantageous features provided by ROS 602 in the preferred embodiment: ... Secure secure communications secure control functions secure virtual memory management information control structures protected from exposure data elements are validated, correlated and access controlled components are encrypted and validated independently components are tightly correlated to prevent unauthorized use of elements control structures and secured executables are validated prior to use to protect against tampering integrates security considerations at the I/O level provides on-the-fly decryption of information at release time enables a secure commercial transaction network flexible key management features" ('193 72:52 - 73:38) 5. "ROS 602 generates component assemblies 690 in a secure matter. As shown graphically in FIGS. 11I and 11J, the different elements comprising a component assembly 690 may be 'interlocking' in the sense that they can only go together in ways that are intended by the VDE participants who created the elements and/or specified the component assemblies. ROS 602 includes security protections that can prevent an unauthorized person from modifying elements, and also prevent an unauthorized person from substituting elements." ('193 84:60 - 85:2) 6. "Because of VDE security, including use of effective encryption, authentication, digital signature, and secure database structures, the records contain within a VDE card arrangement may be accepted as valid transaction records for government and/or corporate recordkeeping requirements." ('193 41:37-42) 7. "In order to maintain security, SPE 503 must encrypt and cryptographically seal each block being swapped out to a storage device external to a supporting SPU 500, and must similarly decrypt, verify the cryptographic seal for, and validate each block as it swapped into SPU 500." ('193 125:60-64) 8. "As mentioned above, memory external to SPU 500 may not be secure. Therefore, when security is required, SPU 500 must encrypt secure information before writing it to external memory before using it." ('193 71:32-36) 9. "Only those processes that execute completely within SPEs 503 (and in some cases, HPEs 655) may be considered to be truly secure. Memory and other resources external to SPE 503 and HPEs 655 used to store and/or process code and/or data to be used in secure processes should only receive and handle that information in encrypted form unless SPE 503/HPE 655 can protect secure process code and/or data form non-secure processes." ('193 81:12-19)

	Claim Term/Phrase	Evidence Supporting MS Construction
		10. "From time to time, two parties (e.g., PPEs A and B), will need to establish a communication channel that is know by both parties to be secure form eavesdropping, secure from tampering, and to be in use solely by the two parties whose identifies are correctly known to each other." ('193 218:33-37) 11. "Since all secure communications are at least in part encrypted and the processing inside the secure subsystem is concealed form outside observation and interference, the present invention ensures that content control information can be enforced." ('193 46:4-8) 12. "VDE 100 provided by the preferred embodiment has sufficient security to help ensure that it cannot be compromised short of a successful 'brute force attack,' and so that the time and cost to succeed in such a 'brute force attack' substantially exceeds any value to be derived. In addition, the security provided by VDE 100 compartmentalizes the internal workings of VDE so that a successful 'brute force attack' would compromise only a strictly bounded subset of protected information, not the entire system." ('193 199:38-47) 13. "Integrity of VDE Security: There are many ways in which a PPE 650 might be compromised. The goal of the security provided by VDE 100 is to reduce the possibility that the system will be compromised, and minimize the adverse effects if it is compromised. The basic cryptographic algorithm that are used to implement VDE 100 are assumed to be safe (cryptographically strong). These include the secret-key encryption of content, public-key signatures for integrity verification, public-key encryption for privacy between PPEs 650 or between a PPE and a VDE administrator, etc. Direct attack on these algorithms is assumed to be beyond the capabilities of an attacker. For domestic versions of VDE 100 some of this probably a safe assumption since the basic building blocks for control information have sufficiently long keys and are sufficiently proven. The following risks of threat or attacks may be significant: Unauthorized creation or modification of component assemblies (e.g., budgets); Unauthorized bulk disclosure of content; Compromise of one or more keys" ('193 221:1-21) 14. See also prior art referenced in the relevant file histories, e.g., Stefik; Tygar et al., "Dyad: A System for Using Physically Secure Coprocessors," School of Computer Science, Carnegie Mellon University, Pittsburgh, PA 15213 (May 1991). 15. "VDE can: (a) audit and analyze the use of content, (b) ensure that content is used only in authorized ways, and (c) allow information regarding content usage to be used only in ways approved by content users." ('193 4:51-56) 16. "Even if the object is stored locally to the VDE node, it may be stored as a secure or protected object so that it is not directly accessible to a calling process." ('193 192:14-17) 17. "An attacker would gain little benefit from intercepting this information since it is transmitted in protected form; she would have to compromise electronic appliance 600(1) or 600(N) (or the SPU 500(1), 500(N)) in order to access this information in unprotected form." ('193 228:25-30) 18. "VDE is a secure system for regulating electronic conduct and commerce. Regulation is ensured by control information put in place by one or more parties." ('193 6:33-35)

	Claim Term/Phrase	Evidence Supporting MS Construction
		19. "It also employs a software object architecture for VDE content containers that carries protected content and may also carry both freely available information (e.g, summary, table of contents) and secured content control information which ensures the performance of control information." ('193 15:41-46) 20. "Because of the breadth of issues resolved by the present invention, it can provide the emerging 'electronic highway' with a single transaction/distribution control system that can, for a very broad range of commercial and data security models, ensure against unauthorized use of confidential and/or proprietary information and commercial electronic transactions." ('193 17:22-28) 21. "VDE can satisfy the requirements of widely differing electronic commerce and data security applications by, in part, employing this general purpose transaction management foundation to securely process VDE transaction related control methods." ('193 25:52-57) 22. "HPE(s) and SPE(s) ... may each perform secure processing based on one or more VDE component assemblies 690, and they may each offer secure processing services to OS kernel 680." ('193 79:41-46) 23. "VDE methods 1000 are designed to provide a very flexible and highly modular approach to secure processing." ('193 181:18-19) 24. "In these cases, secure processing steps performed by an SPU typically must be segmented into small, securely packaged elements that may be 'paged in' and 'paged out' of the limited available internal memory space." (69:43-47) 25. "Summary of Some Important Features Provided by VDE in Accordance With the Present Invention ... VDE employs special purpose hardware distributed throughout some or all locations of a VDE implementation: a) said hardware controlling important elements of: content preparation (such as causing such content to be placed in a VDE content container and associating content control information with said content), content and/or electronic appliance usage auditing, content usage analysis, as well as content usage control; and b) said hardware having been designed to securely handle processing load module control activities, wherein said control processing activities may involve a sequence of required control factors" ('193 21:43 - 22:31) 26. "Memory manager 578 and virtual memory manager 580 in the preferred embodiment manage ROM 532 and RAM 534 memory within SPU 500 in the preferred embodiment. Virtual memory manager 580 provides a fully 'virtual' memory system to increase the amount of 'virtual' RAM available in the SPE secure execution space beyond the amount of physical RAM 534a provided by SPU 500. Memory manager 578 manages the memory in the secure execution space, controlling how it is accessed, allocated and deallocated. SPU MMU 540, if present, supports virtual memory manager 580 and memory manager 578 in the preferred embodiment. In some 'minimal' configurations of SPU 500 there may be no virtual memory capability and all memory management functions will be handled by memory manager 578. Memory management can also be used to help enforce the security provided by SPE 503. In some classes of SPUs 500, for example, the kernel memory manager 578 may use hardware memory management unit (MMU) 540 to provide page level protection within the SPU 500. Such a hardware-based memory management system provides an effective

	Claim Term/Phrase	Evidence Supporting MS Construction
		mechanism for protecting VDE component assemblies 690 from compromise by 'rogue' load modules." ('193 109:24-45) 27. "When a method core 1000' references a load module 1100, a load module is loaded into the SPE 503, decrypted, and then either passed to the electronic appliance microprocessor for executing in an HPE 655 (if that is where it executes), or kept in the SPE (if that is where it executes)." ('193 139:28-31) 28. " The role of go-between 4700 may, in some circumstances, be played by one of the participant's SPU's 500 (PPEs), since SPU (PPE) behavior is not under the user's control, but rather can be under the control of rules and controls provided by one or more other parties other than the user (although in many instances the user can contribute his or her own controls to operate in combination with controls contributed by other parties)." ('683 24:26-33) 29. "Load modules are not necessarily directly governed by PERCs 808 that control them, nor must they contain any time/date information or expiration dates. The only control consideration is the preferred embodiment is that one or more methods 1000 reference them using a correlation tag (the value of a protected object created by the load module's owner, distributed to authorized parties for inclusion in their methods, and to which access and use is controlled by one or more PERCs 808). If a method core 1000' references a load module 1100 and asserts the proper correlation tag (and the load module satisfies the internal tamper checks for the SPE 503), then the load module can be loaded and executed, or it can be acquired from, shipped to, updated, or deleted by, other systems." ('193 139:60 - 140:6) 30. "ROS 602 also provides a tagging and sequencing scheme that may be used within loadable component assemblies 690to detect tampering by substitution. Each element comprising a component assembly 690 may be loaded into a SPU 500, decrypted using encrypt/decrypt engine 522, and then tested/compared to ensure that the proper element has been loaded. ...In addition, a validation/correlation tag stored under the encrypted layer of the loadable element may be compared to make sure it matches on or more tags provided by a requesting process. This prevents unauthorized use of information. As a third protection, a device assigned tag (e.g., a sequence number) stored under an encryption layer of loadable element may be checked to make sure it matches a corresponding tag value expected by SPU 500. This prevents substitution of older elements. Validation/correlation tags are typically passed only in secure wrappers to prevent plaintext exposure of this information outside of SPU 500." ('193 87:41-62) 31. "Key and Tag Manager 558 also provides service relating to tag generation and management. In the preferred embodiment, transaction and access tags are preferably stored by SPE 503 (HPE 665) in protected memory (e.g., within the NVRAM 534b of SPU 500). These tags may be generated by key and tag manager 558. They are used to, for example, check access rights to, validate and correlate data elements. For example, they may be used to ensure components of the secured data structures are not tampered with outside of the SPU 500." ('193 120:59 - 121:1) 32. "Initiation of load module execution in this environment is strictly controlled by a

	Claim Term/Phrase	Evidence Supporting MS Construction
		combination of access tags, validation tags, encryption keys, digital signatures, and/or correlation tags. Thus, a load module 1100 may only be referenced if the caller knows it ID and asserts the shared secret correlation tag specific to that load module. The decrypting SPU may match the identification token an and local access tag of a load module after decryption. These techniques make the physical replacement of any load module 1100 detectable at the next physical access of a load module." ('193 139:45-55) 33. "Meters and budgets are common examples of this. Expiration dates cannot be used effectively to prevent substitution of the previous copy of a budget UDE 1200. To secure these frequently updated items, a transaction tag is generated and included in the encrypted item each time that item is updated. A list of all VDE items Ids and the current transaction tags for each item is maintained as part of the secure database 610." ('193 143:13-20) 34. "UDEs 1200 are preferably encrypted using a site specific key once they are loaded into a site. This site-specific key marks a validation tag that may be derived from a cryptographically strong pseudo-random sequence by the SPE 503 and updated each time the record is written back to the secure database 610. This technique provided reasonable assurance that the UDE 1200 has not been tampered with nor submitted when it is requested by the system for the next use." ('193 143: 29-37) **Extrinsic:** 1. "No data system can be made secure without physical protection of some part of the equipment." (Davies, p. 3) 2. "Security is a negative attribute. We judge a system to be secure if we have not been able to design a method of misusing it which gives some advantage to the attacker." (Davies, p. 4) 3. "Various criteria exist for secure systems - U.S. Dept. of Defense Trusted Computer Security Evaluation Criteria (TCSEC), the Orange Book, Red Book, European and Canadian guidelines, U.S. National Institute of Standards and Technology, and United Kingdom guidelines." (Neumann, p. 233) 4. Security: "1. Protection against unwanted behavior. In present usage, computer security includes properties such as confidentiality, integrity, availability, prevention of denial of service and prevention of generalized misuse. 2. The property that a particular security policy is enforced, with some degree of assurance. 3. Security is sometimes used in the restricted sense of confidentiality, particularly in the case of multilevel security (that is, multilevel confidentiality)." Multilevel Security: "A confidentiality policy based on the relative ordering of multilevel security labels (really multilevel confidentiality, ex. - no adverse flow of information with respect to sensitivity of information)" (Neumann, Glossary and p. 225) 5. "There are two principal objectives: secrecy (or privacy), to prevent unauthorized disclosure of data; and authenticity or integrity) [sic], to prevent the unauthorized modification of data.... Note, however, that whereas it can be used to detect message modification, it cannot prevent it. Encryption alone does not protect against replay, because an opponent could simply replay previous ciphertext."

	Claim Term/Phrase	Evidence Supporting MS Construction
		(Denning, p. 5) 6. "A cipher is unconditionally secure if, no matter how much ciphertext is intercepted, there is not enough information in the ciphertext to determine the plaintext uniquely." (Denning, p. 5) (Davies, pp. 41, 380) 7. "A cipher is computationally secure, or strong, if it cannot be broken by systematic analysis with available resources." (Denning, p. 5) (Davies, pp. 41, 370) 8. Security: "The combination of integrity and secrecy, applied to data." (IT Glossary, 5/12/95, IT00028295) 9. Secrecy: "The inability to obtain any information from data." (IT Glossary, 5/12/95, IT00028294) 10. "… security includes concealment, integrity of messages, authentication of one communicating party by the other…" (Neumann, p. 8) 11. "Computer security rests on confidentiality, integrity, and availability. The interpretations of these three aspects vary, as do the contexts in which they arise. Confidentiality is the concealment of information or resources. … Confidentiality also applies to the existence of data, which is sometimes more revealing than the data itself. … All mechanisms that enforce confidentiality require supporting services from the system. The assumption is that the security services can rely on the kernel, and other agents, to supply correct data. Thus, assumptions and trust underlie the confidentiality mechanisms. Integrity refers to the trustworthiness of data or resources, and it is usually phrased in terms of preventing improper or unauthorized change. Integrity includes data integrity (the content of the information) and origin integrity (the source of the data, often called authentication). Integrity mechanisms fall into two classes: prevention mechanisms and detection mechanisms. Protection mechanisms seek to maintain the integrity of the data by blocking any unauthorized attempts to change the data or any attempts to change the data in unauthorized ways. Detection mechanisms do not try to prevent violations of integrity; they simply report that the data's integrity in no longer trustworthy." (Bishop, pp. 4-6) 12. "Definition 4-1. A security policy is a statement that partitions the states of the system into a set of authorized, or secure, states and a set of unauthorized, or nonsecure, states. A secure system is a system that starts in an authorized state and cannot enter an unauthorized state." (Bishop, p. 95) 13. "24.5.1 Secure Systems Systems designed with security in mind have auditing mechanisms integrated with the system design and implementation." (Bishop, p. 706) 14. "Computer security is assuring the secrecy, integrity, and availability of components of computing systems. The three principal pieces of a computing system subject attacks are hardware, software, and data. These three pieces, and the communications between them, constitute the basis of computer security vulnerabilities. This chapter has identified four kinds of attacks on computing systems: interruptions, interceptions, modifications, and fabrications. Three principles affect the direction of work in computer security. By the principle of easiest penetration, a computing system penetrator will use whatever means of

	Claim Term/Phrase	Evidence Supporting MS Construction
		attack is the easiest; therefore. All aspects of computing system security need to be considered at once. By principle of timeliness, a system needs to be protected against penetration only long enough so that penetration is of no value to the penetrator. The principle of effectiveness states that controls must be usable and used in order to serve purpose. Controls can be applied at the levels of data, programs, the system, physical devices, communications links, the environment, and personnel. Sometimes several controls are needed to cover a single vulnerability, and sometimes one control addresses several problems at once." (Pfleeger, p. 4) 15. See also InterTrust's Rule 30(b)(6) testimony 16. See also Microsoft PLR 4-2 Exhs. E & F as revised, e.g. Webster's (1947), p. 1540-41; Pfleeger, p. 4-5; Spencer, Personal Computer Dictionary, p. 156; The Computer Glossary, p. 460; McGraw-Hill Dictionary of Scientific and Technical Terms, p. 1788; Practical Unix Security (O'Reilly 1991), p. 11-12; Bishop, Computer Security (2002) p. 3-24, 47; Hoffman, Modern Methods for Computer Security and Privacy, p. 134-35; Mullender, ed., Distributed Systems (Addison Wesley 2nd ed.), p. 367, 420; Landewehr, "Formal Models for Computer Security" (ACM 1981); Merkle, "Protocols for Public Key Cryptosystems" (IEEE 1980); Cooper, Computer & Communication Security, p. 383; Baker, The Computer Security Handbook, p. 273; Computer Security Handbook, p. 389; Matheson et al., Robustness and Security of Digital Watermarks; National Information Systems Security (INFOSEC) Glossary, p. 49-50; Internet Security Glossary (RFC2828); Tanenbaum, Modern Operating Systems (1992), p. 181-82; IN64706-45, IN176319-72, IT735936 (integrity), IT735938-9 IN00862862, IT1678-96, IT39208-26, IT702969-83, IT399877-80 17. "Secure. Pertaining to the control of who can use an object and to the extent to which the object can be used by controlling the authority given to the user."; "Computer Security. 1. Concepts, techniques, technical measures, and administrative measures used to protect the hardware, software and data of an information processing system from deliberate or inadvertent unauthorized acquisition, damage, destruction, disclosure, manipulation, modification or use or loss. 2. Protection resulting from the application of computer security." (IBM) 18. "Security: Freedom from risk or danger. Safety and assurance of safety"; "secure state - a condition in which none of the subjects in a system can access objects in an unauthorized manner..." (Russell, pp. 8-11, 113, 227, 420) 19. "The protection of computer hardware and software from accidental or malicious access, use, modification, destruction, or disclosure." (Booth) 20. "Prevention of or protection against (a) access to information by unauthorized recipients or (b) intentional but unauthorized destruction or alteration of that information." (Dictionary of Computing, p. 406)

	Claim Term/Phrase	Evidence Supporting MS Construction
		21. "The quality or state of being cost-effectively protected from undue losses (e.g. loss of goodwill, monetary loss, loss of ability to continue operations, etc.)" (Longley). 22. Hoffman, Modern Methods for Computer Security & Privacy, p. 134 23. "Protected Location: A memory location that can only be accessed by an authorized user or process."; "Protected domain: A set of access privileges to protected resources." (Dictionary of Computing) 24. Protect: "To prevent unauthorized access to programs or a computer system; to shield against harm." (Webster's) 25. Protection: "(1) (computing systems). See: Storage protection (2) (software). An arrangement for restricting access to or use of a all, or part, of a computer system."; Storage protection: "An arrangement for preventing access to storage for either reading or writing, or both." (Booth) 26. IN00862862 27. Security: "The combination of integrity and secrecy, applied to data." (IT Glossary, 5/12/95, IT00028295) 28. "Secrecy: The inability to obtain any information from data." (IT Glossary, 5/12/95, IT00028294) 29. Processing: "1. The performance of logical operations and calculations on datum including temporary retention of data in processor storage while the data is being operated on." (IBM) 30. Process: "(1) in computing, the active system entity through which programs run. The entity in a computer system to which authorizations are granted; thus the unit of accountability in a computer system. (2) In computing, a program in execution.... (4) In computing, a program is a static piece of code and a process is the execution of that code." (Longley) 31. Processing: "In legislation, as defined by the U.K. Data Protection Act of 1984, pertaining to the amending, augmenting, deleting, or re-arranging of the data or extracting the information constituting the data and, in the case of personal data, processing means performing any of the abovementioned operations by reference to the data subject." (Longley)
20.	secure container 683.2 861.58 912.35	**Intrinsic:** 1. "Anderson [U.S. Patent No. 5,537,526] does not explicitly address a secure container *per se*, but does place documents into containers [Fig. 8 202] and place restriction via links attached to documents ... which can include restrictions ... Such security tools are rightfully attached to a structure encapsulating the document, e.g. its container." (Prosecution History for the 08/805,804 Patent Application (issued as the '861), Office Action, 6/25/98, p. 5 (MSI 27417-25)) 2. "Claims 7-11, ... are rejected under 35 U.S.C. 103(a) as being unpatentable over Fischer (5,412,717) in view of Narasimhalu et al (5,499,298). ... The set of authorities and restrictions are referred to as 'program authorization information' or 'PAI'. ... A comparison of independent claim 7 to Fischer to derive the similarities and differences between the claimed invention and the prior art follows. ... Here, Fischer provides a secure container in the form of a program, i.e. a governed item, having an associated PAI, i.e. at least one rule associated with the secure container." (Prosecution History for the 09/221,479 Patent

	Claim Term/Phrase	Evidence Supporting MS Construction
		Application (issued as the '683), Office Action, 11/12/99, pp. 3-4 (IT00065799-800)) 3. "1. (Amended) A rights management method comprising: (a) receiving an information signal; (b) steganographically decoding the received information signal to recover digital rights management control information <u>packaged within at least one secure digital container;</u> and (c) performing at least one rights management operation based at least in part on the recovered digital rights management control information. … Remarks … For example, amended Claims 1, 15 and 22 each recite a digital secure container in combination. Neither Rhoads [U.S. Patent No. 5,636,292], nor any of the other applied references, teaches or suggests the recited combination of features including any digital secure container." (Prosecution History for the 08/689,606 Patent Application filed 8/12/96) (issued as U.S. Patent 5,943,422, incorporating '107), Amendment, 7/2/98, pp. 1-2, 101 (MSI188164-165, MSI188264) 4. Rhoads, U.S. Patent No. 5,636,292: a. "Fully Exact Steganography Prior art steganographic methods currently known to the inventor generally involve fully deterministic or 'exact' prescriptions for passing a message. Another way to say this is that it is a basic assumption that for a given message to be passed correctly in its entirety, the receiver of the information needs to receive the exact digital data file sent by the sender, tolerating no bit errors or 'loss' of data. By definition, 'lossy' compression and decompression on empirical signals defeat such steganographic methods. (Prior art, such as the previously noted Komatsu work, are the exceptions here.) The principles of this invention can also be utilized as an exact form of steganography proper. It is suggested that such exact forms of steganography, whether those of prior art or those of this invention, be combined with the relatively recent art of the 'digital signature' and/or the DSS (digital signature standard) in such a way that a receiver of a given empirical data file can first verify that not one single bit of information has been altered in the received file, and thus verify that the contained exact steganographic message has not been altered." (Rhoads 55:5-26) b. "One exemplary application is placement of identification recognition units directly within modestly priced home audio and video instrumentation (such as a TV). Such recognition units would typically monitor 'audio and/or video looking for these copyright identification codes, and thence triggering simple decisions based on the findings, such as disabling or enabling recording capabilities, or incrementing program specific billing meters which are transmitted back to a central audio/video service provider and placed onto monthly invoices." (Rhoads 29:23-33) 5. "Use of secure electronic containers to transport items provides an unprecedented degree of security, trustedness and flexibility." ('683 8:50-52) 6. "Even if the object is stored locally to the VDE node, it may be stored as a secure or protected object so that it is not directly accessible to a calling process. ACCESS method 2000 establishes the connections, routings, and security

	Claim Term/Phrase	Evidence Supporting MS Construction
		requisites needed to access the object." ('193 192:14-19) 7. "Electronic delivery person 4060 receives item 4054 in digital form and places it into a secure electronic container 302–thus forming a digital 'object' 300. A digital object 300 may in this case be, for example, as shown in FIGS. 5A and 5B, and may include one or more containers 302 containing item 4054. FIG. 88 illustrates secure electronic container 302 as an attaché case handcuffed to the secure delivery person's wrist. Once again, container is shown as a physical thing for purposes of illustration only--in the example it is preferably electronic rather than physical, and comprises digital information having a well-defined structure (see FIG. 5A). Special mathematical techniques known as 'cryptography' can be used to make electronic container 302 secure so that only intended recipient 4056 can open the container and access the electronic document (or other item) 4054 it contains." ('683 15:56 - 16:6) 8. "[C]ontainer 152 can only be opened within a secure protected processing environment 154 that is part of the virtual distribution environment described in the above-referenced Ginter et al. patent disclosure ...." ('712 168:22-25) 9. "A VDE content container is an object that contains both content (for example, commercially distributed electronic information products such as computer software programs, movies, electronic publications or reference materials, etc.) and certain control information related to the use of the object's content." ('193 19:15-21) 10. "Other applications, such as application 608b shown in FIG. 11B, may not be 'VDE Aware' and therefore may not 'know' how to directly access an interface to VDE functions 604 provided by API 682. To provide for this, ROS 602 may include a 'redirector' 684 that allows such 'non- VDE aware' applications 608(b) to access VDE objects 300 and functions 604. Redirector 684, in the preferred embodiment, translates OS calls directed to the 'other OS functions' 606 into calls to the 'VDE functions' 604. As one simple example, redirector 684 may intercept a 'file open' call from application 608(b), determine whether the file to be opened is contained within a VDE container 300, and if it is, generate appropriate VDE function call(s) to file system 687 to open the VDE container (and potentially generate events to HPE 655 and/or SPE 503 to determine the name(s) of file(s) that may be stored in a VDE object 300, establish a control structure associated with a VDE object 300, perform a registration for a VDE object 300, etc.). Without redirector 684 in this example, a non-VDE aware application such as 608b could access only the part of API 682 that provides an interface to other OS functions 606, and therefore could not access any VDE functions." ('193 82:24-45) 11. "ACCESS method 2000 reads the ACCESS method MDE from the secure database, reads it in accordance with the ACCESS method DTD, and loads encrypted content source and routing information based on the MDE (blocks 2010, 2012). This source and routing information specifies the location of the encrypted content. ACCESS method 2000 then determines whether a connection to the content is available (decision block 2014). This 'connection' could be, for example, an on-line connection to a remote site, a real-time information feed, or a path to a secure/protected resource, for example. If the connection to the content

	Claim Term/Phrase	Evidence Supporting MS Construction
		is not currently available ('No' exit of decision block 2014), then ACCESS method 2000 takes steps to open the connection (block 2016). If the connection fails (e.g., because the user is not authorized to access a protected secure resource), then the ACCESS method 2000 returns with a failure indication (termination point 2018)." ('193 192:36-52) 12. "Appliance 600B may deliver the digital copy of item 4054 within a container 302 and/or may protect the item with seals, electronic fingerprints, watermarks and/or other visible and/or hidden markings to provide a 'virtual container' or some of the security or other characteristics of a container (for example, the ability to associate electronic controls with the item)." ('683 18:49-56) 13. "Trade-offs between flexibility, ease of use and incompatibility and interoperability can be further complicated when security considerations come into play. To be effective in many electronic commerce applications, electronic container designs should be tamper-resistant and secure. One must assume that any tools widely used to create and/or use containers will fall into the hands of those trying to break or crack open the containers or otherwise use digital information without authorization. Therefore, the container creation and usage tools must themselves be secure in the sense that they must protect certain details about the container design. This additional security requirement can make it even more difficult to make containers easy to use and to provide interoperability." ('861 4:51-64) **Extrinsic:** 1. Container: "VDE objects are represented in a special form called a container. The container is implemented within the VDE as an object-oriented container class. The container class provides a standard method by which applications software may encapsulate and read information stored within the object. Additionally, the container may include procedural information associated with the data being stored. Containers may be nested, and share attributes with nested elements. Nested containers are stored within a larger container. VDE recognizes the presence of additional objects within the content, and allows the nested containers to share, extend or override the attributes of an outer container." (VDE ROI DEVICE v1.0a, 2/9/94, IT00008572) 2. Secure: "Pertaining to the control of who can use an object and to the extent to which the object can be used by controlling the authority given to the user." (IBM) 3. Container: "In data security, a multilevel information structure. A container has a classification and may contain objects and/or other containers." (Longley) 4. Container: "A protected (encrypted) storage object that incorporates descriptive information, protected content, and (optionally) control objects applicable to that content." (IT Glossary, 3/7/95, IT00709617) 5. Container: "A contains protected *content*, which is divided into one or more *atomic elements*, and, optionally, *PERCs* governing the *content* and may be manipulated only as specified by a *PERC.*" (IT Glossary, 4/6/95, IT00028206) 6. Container: "A packaging mechanism, consisting of: *One or more Element-derived components. *An organization mechanism which provides a unique name

	Claim Term/Phrase	Evidence Supporting MS Construction
		within a flat namespace for each of the components in a Container." (IT Glossary, 5/12/95, IT00028293) 7. Container: "A protected digital information storage and transport mechanism for packaging content and control information." (IT Glossary, 8/21/95, TD00068B, IT00032372) 8. Secure container: "'Secure Container(s)' means electronic container(s) or electronic data arrangements that: (I) use one or more cryptographic or other obfuscation techniques to provide protection for at least a portion of the Content thereof; and (ii) supports the use of Rules and Controls to enable the Management of Content." (License Agreement IT and Universal Music Group, 4/13/99, Exhibit 11 to IT 30(b)(6)) 9. Secure container: "A DigiBox container provides security through encryption and the PPE of a commerce node. A secure container does not require a secure communications transport mode." (IT00035965) 10. "A DigiBox container provides for the persistent protection of its properties." (IT 00035920) 11. "DigiBox containers ensure integrity." (IT00035895)
21.	tamper resistance 721.1	**Intrinsic:** 1. "The level of security and tamper resistance required for trusted SPU hardware processes depends on the commercial requirements of particular markets or market niches, and may vary widely." ('193 49:59-62) **Extrinsic:** 1. Tamper-resistant Module: "In data security, a device in which sensitive information, such as a master cryptographic key, is stored and cryptographic functions are performed. The device has one or more sensors to detect physical attacks, by an adversary trying to gain access to the stored information in which case the stored sensitive data is immediately destroyed." (Longley) 2. See also IT41530-49, IT51147-60 3. "Subversion: A compromise that undermines integrity." (Neumann, p. 349) 4. "Spoofing: Taking on the characteristics of another system or used for purposes of deception. In the present contexts, spoofing is generally prankish rather than overtly malicious, although it is often used elsewhere in a malicious contexts." (Neumann, p. 349) 5. Security: "1. Protection against unwanted behaviors. In present usage, computer security includes properties such as confidentiality, integrity, availability, prevention of denial of service, and prevention of generalized misuse. 2. The property that a particular security policy is enforced, with some degree of assurance. 3. Security is sometimes used in the restricted sense of confidentiality, particularly in the case of multilevel security (that is, multilevel confidentiality)." (Neumann, p. 349)
22.	tamper resistant barrier 721.34	**Intrinsic:** 1. "In addition, Applicants would like to draw the Examiner's attention to other sections of the specification in support of words or phrases cited by the Examiner as 'indefinite.' … In claims … 36 … the term 'barrier' is used as part of the phrase 'tamper resistant barrier.' This phrase is described in the specification on

	Claim Term/Phrase	Evidence Supporting MS Construction
		at least pages 7-8 and 46. In addition, the incorporated Ginter application describes tamper resistant barriers in a number of locations such as, for example, page 201." (Prosecution History for the 08/689,754 Patent Application (issued as the '721), Amendment, 4/14/99, p. 14.) (p. 7 and 46 of the original specification are '721 2:62 - 3:13 and 16:35-54 of the issued patent; p. 201 of Ginter application 08/388,107 is '193 80:40 - 81:1) 2. "SPU 500 is enclosed within and protected by a 'tamper resistant security barrier' 502. Security barrier 502 separates the secure environment 503 from the rest of the world. It prevents information and processes within the secure environment 503 from being observed, interfered with and leaving except under appropriate secure conditions." ('193 59:48-53) 3. "Although block 1262 includes encrypted summary services information on the back up, it preferably does not include SPU device private keys, shared keys, SPU code and other internal security information to prevent this information from ever becoming available to users even in encrypted form." ('193 166:59-64) 4. "Briefly, the preferred example software-based PPE 650 installation process provides the following security techniques: encrypted software distribution, installation customized on a unique instance and/or electronic appliance basis, encrypted on-disk form, installation tied to payment method, unique software and data layout, and identifiable copies.". ('900 236:32-42) 5. "... (c) if the load module has an associate digital signature , authenticating the digital signature at least one public key secured behind a tamper resistant barrier and therefore hidden from the user." ('721 22:5-16 (claim 9)) 6. "A further attack technique might involve duplicating one installed operational material 3472 instance by coping the programs and data from one personal computer 3372B to another personal computer 3372C or emulator (see FIG. 67B, block 3364, and the 'copy' arrow 3364A in FIG. 67A). The duplicated PPE instance could be used in a variety of ways, such as, for example, to place an imposter PPE 650 instance on-line and/or to permit further dynamic analysis." ('900 233:8-15) 7. "Various software protection techniques detailed above in connection with FIG. 10 may provide software-based tamper resistant barrier 674 within a software-only and/or hybrid software/hardware protected processing environment 650. The following is an elaboration on those above-described techniques. These software protection techniques may provide, for example, the following: An on-line registration process that results in the creation of a shared secret between the registry and the PPE 650 instance—used by the registry to create content and transactions that are meaningful only to specific PPE instance. An installation program (that may be distinct from the PPE operational material software) that creates a customized installation of the PPE software unique to each PPE instance and/or associate electronic appliance 600. Camouflage protections that make it difficult to reverse engineer the PPE 650 operational materials during PPE 650 operation. Integrity checks performed during PPE 650 operation (e.g., during on-line interactions with trusted servers) to detect compromise. In general, the software-based tamper resistant barrier 674 may establish 'trust' primarily through uniqueness and complexity." ('900 235:30-57)

	Claim Term/Phrase	Evidence Supporting MS Construction
		8. "Operational materials 3472 may then decrypt the next program segment dynamically … This mechanism increases the tamper-resistant of the executable code-- thus providing additional tamper resistance for PPE operations." ('900 243:3-9) 9. "The software-based tamper resistant barrier 674 provided by HPE 655 may be provided, for example, by: introducing time checks and/or code modifications to complicate the process of stepping through code comprising a portion of kernel 688a and/or a portion of component assemblies 690 using a debugger; using a map of defects on a storage device (e.g., a hard disk, memory card, etc.) to form internal test values to impede moving and/or copying HPE 655 to other electronic appliances 600; using kernel code that contains false branches and other complications in flow of control to disguise internal processes to some degree from disassembly or other efforts to discover details of processes; using 'self-generating' code (based on the output of a co-sine transform, for example) such that detailed and/or complete instruction sequences are not stored explicitly on storage devices and/or in active memory but rather are generated as needed; using code that 'shuffles' memory locations used for data values based on operational parameters to complicate efforts to manipulate such values; using any software and/or hardware memory management resources of electronic appliance 600 to 'protect' the operation of HPE 655 from other processes, functions, etc. Although such a software-based tamper resistant barrier 674 may provide a fair degree of security, it typically will not be as secure as the hardware-based tamper resistant barrier 502 provided (at least in part) by SPU 500." ('193 80:40-65, Fig. 10) 10. "Software-based tamper resistant barrier 674 may be created by software executing on a general-purpose CPU. Various software protection techniques may be used to construct and/or provide software-based tamper resistant barrier 674." ('900 230:61-65) 11. "No software-only tamper resistant barrier 674 can be wholly effective against all of these threats. A sufficiently powerful dynamic analysis (such as one employing an in-circuit emulator) can lay bare all of the software-based PPE 650's secrets. Nonetheless, various techniques described below in connection with FIG. 69A and following make such an analysis extremely frustrating and time consuming--increasing the 'work factor' to a point where it may become commercially unfeasible to attempt to 'crack' a software-based tamper resistant barrier 674." ('900 233:24-33) 12. "For example, the PPE 650 may rewrite or overwrite memory locations immediately after using same to make their contents unavailable for scrutiny. Similarly, the PPE 650 operational software may use hardware and/or time dependent sequences to prevent emulation. Additionally, some of the PPE 650 environment code may be self-modifying." ('900 236:9-15) **Extrinsic:** 1. Tamper-resistant module: "In data security, a device in which sensitive information, such as a master cryptographic key, is stored and cryptographic functions are performed. The device has one or more sensors to detect physical attacks, by an adversary trying to gain access to the stored information in which

	Claim Term/Phrase	Evidence Supporting MS Construction
		case the stored sensitive data is immediately destroyed." (Longley) 2. "The 'tamper-resistant module' is physically strong and destroys secrets when opened, and the software running inside has been checked for integrity;" (Davies, p. 3) 3. "The host computer is provided with a specially, physically secure module containing all the secret information which must be protected. In the IBM papers it is called the 'Cryptographic Facility': we shall call it a 'Tamper Resistant Module' (TRM)." (Davies, p. 144)
23.	use 193.19 683.2 721.1 861.58 891.1 912.8, 912.35	**Intrinsic:** 1. "Provides non-repudiation of use and may record specific forms of use such as viewing, editing, extracting, copying, redistributing (including to what one or more parties), and/or saving." ('683 6:46-48) 2. "Content (executables for example) delivered with proof of delivery and/or execution or other use." ('683 7:8-9) 3. "In general, VDE enables parties that (a) have rights in electronic information, and/or (b) act as direct or indirect agents for parties who have rights in electronic information, to ensure that the moving, accessing, modifying, or otherwise using of information can be securely controlled by rules regarding how, when, where, and by whom such activities can be performed." ('193 6:24-31) 4. "Some or all of the back up files may be packaged within an administrative object and transmitted for analysis, transportation, or other uses." ('193 167:45-48) 5. "to securely control access and other use, including distribution of records, documents, and notes associated with the case." ('193 274:34-36) 6. "Thus wrapped, a VDE object may be distributed to the recipient without fear of unauthorized access and/or other use. The one or more authorized users who have received an object are the only parties who may open that object and view and/or manipulate and/or otherwise modify its contents and VDE secure auditing ensures a record of all such user content activities." ('193 277:15-21) 7. "These appliances typically include a secure subsystem that can enable control of content use such as displaying, encrypting, decrypting, printing, copying, saving, extracting, embedding, distributing, auditing usage, etc." ('193 9:24-27) 8. "VDE provides a secure, distributed electronic transaction management system for controlling the distribution and/or other usage of electronically provided and/or stored information." ('193 9:36-39) 9. "As a result, VDE supports most types of electronic information and/or appliance: usage control (including distribution), security, usage auditing, reporting, other administration, and payment arrangements." ('193 13:50-53) 10. "SPU 500 is enclosed within and protected by a 'tamper resistant security barrier' 502. Security barrier 502 separates the secure environment 503 from the rest of the world. It prevents information and processes within the secure environment 503 from being observed, interfered with and leaving except under appropriate secure conditions. Barrier 502 also controls external access to secure resources, processes and information within SPU 500. In one example, tamper resistant security barrier 502 is formed by security features such as 'encryption,' and hardware that detects tampering and/or destroys sensitive information within secure environment 503 when tampering is detected." ('193 59:48-59)

	Claim Term/Phrase	Evidence Supporting MS Construction
		11. "Once the information is downloaded, the now-initialized PPE 650 can discard (or simply not use) the manufacturing key." ('193 212:57-59) **Extrinsic:** 1. User: "A person using a InterTrust node to perform some function (i.e., acting in some role). A user is identified with respect to the node by a user ID." (IT Glossary, 5/12/95, IT00028300) 2. User ID: "Locally to a InterTrust node, each InterTrust user has an ID associated with a user name and authentication (e.g., password). In some deployments, there may be only one user, and access to the machine may be considered sufficient authentication; in such cases, the user ID concept may not be visible to the user even though it is present in the implementation." (IT Glossary, 5/12/95, IT00028301) 3. Use: "To use an object is to access the content. This involves the processes of controlling and metering the use of the property and creating audit trail records on the use." (VDE ROI DEVICE v1.0a, 2/9/94, IT00008570)
24.	virtual distribution environment 900.155 Also as set forth in each "claim as a whole" by Microsoft.	Virtual Distribution Environment: "CLAIM AS A WHOLE": **Intrinsic:** 1. "The instant application is one of a series of applications which are all generally directed to a virtual distribution environment." (09/208,017 ('193), Examiner's Amendment, 8/4/00, p. 2) 2. See generally Background and Summary of Invention of '193 Patent ('193 2:22 - 49:63) 3. "With respect to the remaining issues, Applicants respectfully disagree. For example, the Examiner objects to the use of 'environment' as indefinite and unclear. This word, however, is not used in isolation, but rather in the context of several longer phrases, all of which are defined in the specification. The phrase 'protected processing environment,' for example, is used in Claims 11 and 15-18 and described on at least, for example, pages 7-8 and 25 of the specification. The term 'virtual distribution environment' used in Claim 11 is described, for example, on page 7 of the specification. The terms are also described in the commonly copending application Serial Number 08/388,107 of Ginter et al., filed 13 February 1995, entitled 'System and Methods for Secure Transaction Management and Electronic Rights Protection.' A copy of the incorporated Ginter application can be provided to the Examiner upon request." 08/689,754 ('721), Amendment, 4/14/99, p. 13 (pp. 7, 7-8 and 25 of the original specification are '721 2:62 - 3:13, 2:62 - 3:34 and 8:6-28 of the issued patent) 4. See also, Prosecution History of '900: Claims 302, 321 and 322, as pending: "302. A virtual distribution environment comprising • a first host processing environment comprising • a central processing unit;

	Claim Term/Phrase	Evidence Supporting MS Construction
		• main memory operatively connected to said central processing unit; • mass storage operatively connected to said central processing unit and said main memory; • said mass storage storing tamper resistant software designed to be loaded into said main memory and executed by said central processing unit, said tamper resistant software comprising: • machine check programming which derives information from one or more aspects of said host processing environment, • one or more storage locations storing said information; and • integrity programming which • causes said machine check programming to derive said information, • compares said information to information previously stored in said one or more storage locations, and • generates an indication based on the result of said comparison. 321. A virtual distribution environment as in claim 302, • said virtual distribution environment further comprising programming which takes one or more actions based on the state of said indication. 322. A virtual distribution environment as in claim 321 in which said one or more actions includes at least temporarily halting further processing." (Prosecution History for Patent Application 08/706,206 (issued as the '900 patent), Amendment, 06/09/98, 92-93, 96, 96-97)) b. "Claims … 322-324, … are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims." (Prosecution History for Patent Application 08/706,206, Office Action, 08/27/98, p. 2) c. "322. A virtual distribution environment comprising • a first host processing environment comprising • a central processing unit; • main memory operatively connected to said central processing unit; • mass storage operatively connected to said central processing unit and said main memory; • said mass storage storing tamper resistant software designed to be loaded into said main memory and executed by said central processing unit, said tamper resistant software comprising: • machine check programming which derives information from one or more aspects of said host processing environment, • one or more storage locations storing said information; • integrity programming which o causes said machine check programming to derive said information, o compares said information to information previously stored in said one or more storage locations, and o generates an indication based on the result of said comparison; and • programming which takes one or more actions based on the state of

	Claim Term/Phrase	Evidence Supporting MS Construction
		said indication; • said one or more actions including at least temporarily halting further processing." ... Remarks, "Applicants appreciate the indication that claims … are allowed and that claims … 322-324 are objected to but would be allowable if rewritten into independent form. … For purposes of expedition, applicants are cancelling the rejected claims without prejudice …, and are rewriting objected to dependent claims into independent form." (Prosecution History for Patent Application 08/706,206, Amendment, 11/23/98, p. 27-28, 42) (1) DATA SECURITY AND COMMERCE WORLD: **Intrinsic:** 1. "VDE supports a model wide, distributed security implementation which creates a single secure 'virtual' transaction processing and information storage environment. VDE enables distributed VDE installations to securely store and communicate information and remotely control the execution processes and the character of use of electronic information at other VDE installations and in a wide variety of ways. . . " ('193 21:57-65) 2. "The rights protection problems solved by the present invention are electronic versions of basic societal issues. These issues include protecting property rights, protecting privacy rights, properly compensating people and organizations for their work and risk, protecting money and credit, and generally protecting the security of information." ('193 4:8-13) 3. "The present invention provides a new kind of 'virtual distribution environment' (called 'VDE' in this document) that secures, administers, and audits electronic information use. VDE also features fundamentally important capabilities for managing content that travels 'across' the 'information highway.'" ('193 2:24-28) 4. "A fundamental problem for electronic content providers is extending their ability to control the use of proprietary information. Content providers often need to limit use to authorized activities and amounts. Participants in a business model involving, for example, provision of movies and advertising on optical discs may include actors, directors, script and other writers, musicians, studios, publishers, distributors, retailers, advertisers, credit card services, and content end-users. These participants need the ability to embody their range of agreements and requirements, including use limitations, into an 'extended' agreement comprising an overall electronic business model. This extended agreement is represented by electronic content control information that can automatically enforce agreed upon rights and obligations. Under VDE, such an extended agreement may comprise an electronic contract involving all business model participants. Such an agreement may alternatively, or in addition, be made up of electronic agreements between subsets of the business model participants. Through the use of VDE, electronic commerce can function in the same way as traditional commerce-that

	Claim Term/Phrase	Evidence Supporting MS Construction
		is commercial relationships regarding products and services can be shaped through the negotiation of one or more agreements between a variety of parties." ('193 2:37-60) 5. "Protecting the rights of electronic community members involves a broad range of technologies. VDE combines these technologies in a way that creates a 'distributed' electronic rights protection 'environment.' This environment secures and protects transactions and other processes important for rights protection. VDE, for example, provides the ability to prevent, or impede, interference with and/or observation of, important rights related transactions and processes." ('193 3:63 - 4:3) 6. "VDE is a cost-effective and efficient rights protection solution that provides a unified, consistent system for securing and managing transaction processing. VDE can: (a) audit and analyze the use of content, (b) ensure that content is used only in authorized ways, and (c) allow information regarding content usage to be used only in ways approved by content users." ('193 4:48-55) 7. "In general, VDE enables parties that (a) have rights in electronic information, and/or (b) act as direct or indirect agents for parties who have rights in electronic information, to ensure that the moving, accessing, modifying, or otherwise using of information can be securely controlled by rules regarding how, when, where, and by whom such activities can be performed." ('193 6:24-30) 8. "A variety of capabilities are required to implement an electronic commerce environment. VDE is the first system that provides many of these capabilities and therefore solves fundamental problems related to electronic dissemination of information." ('193 8:16-20) 9. "VDE offers an architecture that avoids reflecting specific distribution biases, administrative and control perspectives, and content types. Instead, VDE provides a broad-spectrum, fundamentally configurable and portable, electronic transaction control, distributing, usage, auditing, reporting, and payment operating environment. VDE is not limited to being an application or application specific toolset that covers only a limited subset of electronic interaction activities and participants. Rather, VDE supports systems by which such applications can be created, modified, and/or reused. As a result, the present invention answers pressing, unsolved needs by offering a system that supports a standardized control environment which facilitates interoperability of electronic appliances, interoperability of content containers, and efficient creation of electronic commerce applications and models through the use of a programmable, secure electronic transactions management foundation and reusable and extensible executable components. VDE can support a single electronic 'world' within which most forms of electronic transaction activities can be managed." ('193 8:53 - 9:5) 10. "VDE can securely manage the integration of control information provided by two or more parties. As a result, VDE can construct an electronic agreement between VDE participants that represent a 'negotiation' between, the control requirements of, two or more parties and enacts terms and conditions of a resulting agreement. VDE ensures the rights of each party to an electronic agreement regarding a wide range of electronic activities related to electronic

	Claim Term/Phrase	Evidence Supporting MS Construction
		information and/or appliance usage." ('193 9:52-61) 11. "'Hardware' 506 also contains long-term and short-term memories to store information securely so it can't be tampered with." ('193 60:1-3) 12. "VDE prevents many forms of unauthorized use of electronic information, by controlling and auditing (and other administration of use) electronically stored and/or disseminated information." ('193 11:60-63) 13. "Together, these VDE components comprise a secure, virtual, distributed content and/or appliance control, auditing (and other administration), reporting, and payment environment." ('193 13:14-17) 14. "VDE can securely deliver information from one party to another concerning the use of commercially distributed electronic content. Even if parties are separated by several 'steps' in a chain (pathway) of handling for such content usage information, such information is protected by VDE through encryption and/or other secure processing. Because of that protection, the accuracy of such information is guaranteed by VDE, and the information can be trusted by all parties to whom it is delivered." ('193 14:31-39) 15. "VDE allows the needs of electronic commerce participants to be served and it can bind such participants together in a universe wide, trusted commercial network that can be secure enough to support very large amounts of commerce. VDE's security and metering secure subsystem core will be present at all physical locations where VDE related content is (a) assigned usage related control information (rules and mediating data), and/or (b) used. This core can perform security and auditing functions (including metering) that operate within a 'virtual black box,' a collection of distributed, very secure VDE related hardware instances that are interconnected by secured information exchange (for example, telecommunication) processes and distributed database means." ('193 15:14-27) 16. "VDE provides organization, community, and/or universe wide secure environments whose integrity is assured by processes securely controlled in VDE participant user installations (nodes)." ('193 20:48-51) 17. "Summary of Some Important Features Provided by VDE in Accordance With the Present Invention: VDE employs a variety of capabilities that serve as a foundation for a general purpose, sufficiently secure distributed electronic commerce solution. VDE enables an electronic commerce marketplace that supports divergent, competitive business partnerships, agreements, and evolving overall business models. For example, … employ 'templates' to ease the process of configuring capabilities of the present invention as they relate to specific industries or businesses…. Given the very large range of capabilities and configurations supported by the present invention, reducing the range of configuration opportunities to a manageable subset particularly appropriate for a given business model allows the full configurable power of the present invention to be easily employed by 'typical' users who would be otherwise burdened with complex programming and/or configuration design responsibilities template applications can also help ensure that VDE related processes are secure and optimally bug free by reducing the risks associated with the contribution of independently developed load modules, including unpredictable aspects of code interaction between independent modules and applications, as well as security

	Claim Term/Phrase	Evidence Supporting MS Construction
		risks associated with possible presence of viruses in such modules.... As the context surrounding these templates changes or evolves, template applications provided under the present invention may be modified to meet these changes for broad use, or for more focused activities .... Of course, templates may, under certain circumstances have fixed control information and not provide for user selections or parameter data entry." ('193 21:43-53; 27:1 - 28:18) 18. "Summary of Some Important Features Provided by VDE in Accordance With the Present Invention:... provide mechanisms to persistently maintain trusted content usage and reporting control information through both a sufficiently secure chain of handling of content and content control information and through various forms of usage of such content wherein said persistence of control may survive such use. Persistence of control includes the ability to extract information from a VDE container object by creating a new container whose contents are at least in part secured and that contains both the extracted content and at least a portion of the control information which control information of the original container and/or are at least in part produced by control information of the original container for this purpose and/or VDE installation control information stipulates should persist and/or control usage of content in the newly formed container. Such control information can continue to manage usage of container content if the container is 'embedded' into another VDE managed object, such as an object which contains plural embedded VDE containers, each of which contains content derived (extracted) from a different source." ('193 21:43-45; 28:45-65) 19. "Summary of Some Important Features Provided by VDE in Accordance With the Present Invention ... Interoperability is fundamental to efficient electronic commerce. The design of the VDE foundation, VDE load modules, and VDE containers, are important features that enable the VDE node operating environment to be compatible with a very broad range of electronic appliances." ('193 21:43-45; 34:25-30) 20. "Summary of Some Important Features Provided by VDE in Accordance With the Present Invention ... securely support electronic currency and credit usage control, storage, and communication at, and between, VDE installations." ('193 21:43-45; 36:49-51) 21. "Summary of Some Important Features Provided by VDE in Accordance With the Present Invention ... requiring reporting and payment compliance by employing exhaustion of budgets and time ageing of keys." ('193 21:43-45; 40:8-9) 22. "Summary of Some Important Features Provided by VDE in Accordance With the Present Invention ... Because of the VDE security, including use of effective encryption, authentication, digital signaturing, and secure database structures, the records contained within a VDE card arrangement may be accepted as valid transaction records for government and/or corporate recordkeeping requirements." ('193 21:43-45; 41:37-42) 23. "Since all secure communications are at least in part encrypted and the processing inside the secure subsystem is concealed from outside observation and interference, the present invention ensures that content control information can be enforced." ('193 46:4-8)

	Claim Term/Phrase	Evidence Supporting MS Construction
		24. "An important feature of VDE is that it can be used to assure the administration of, and adequacy of security and rights protection for, electronic agreements implemented through the use of the present invention." ('193 46:51-54) 25. "These are merely a few simple examples demonstrating the importance of ROS 602 ensuring that certain component assemblies 690 are formed in a secure manner. ROS 602 provides a wide range of protections against a wide range of 'threats' to the secure handling and execution of component assemblies 690." ('193 85:15-20) 26. "VDE further enables this process by providing a secure execution space in which the negotiation process(es) are assured of integrity and confidentiality in their operation." ('193 245:20-22) 27. "Taken together, and employed at times with VDE administrative objects and VDE security arrangements and processes, the present invention truly achieves a content control and auditing architecture that can be configured to most any commercial distribution embodiment." ('193 261:10-15) 28. "For example, VDE 100 positively controls content access and usage, provides guarantee of payment for content used, and enforces budget limits for accessed content." ('193 240:53-56) 29. "Such metering is a flexible basis for ensuring payment for content royalties, licensing, purchasing, and/or advertising." ('193 33:56-58) 30. "The overall integrity and security of VDE 100 could ensure, in a coherent and centralized manner, that electronic reporting of tax related information (derived from one or more electronic commerce activities) would be valid and comprehensive." ('193 237:47-51) 31. "Distributors 106 and financial clearinghouses 116 may themselves be audited based on secure records of their administrative activities and a chain of reliable, 'trusted' processes ensures the integrity of the overall digital distribution process. This allows content owners, for example, to verify that they are receiving appropriate compensation based on actual content usage or other agreed-upon bases." ('193 254:66 - 255:5) 32. "Because the control information is carried with each copy of a VDE protected document, and can ensure that central registries are updated and/or that originators are notified of document use, tracking can be prompt and accurate." ('193 281:14-16) 33. "A final desirable feature of agreements in general (and electronic representations of agreements in particular) is that they be accurately recorded in a non-repudiatable form. In traditional terms, this involves creating a paper document (a contract) that describes the rights, restrictions, and obligations of all parties involved. This document is read and then signed by all parties as being an accurate representation of the agreement. Electronic agreements, by their nature, may not be initially rendered in paper. VDE enables such agreements to be accurately electronically described and then electronically signed to prevent repudiation." ('193 245:25-35) 34. "As discussed above, a wide variety of techniques are currently being used to provide secure, trusted confidential delivery of documents and other items. Unfortunately, none of these previously existing mechanisms provide truly

	Claim Term/Phrase	Evidence Supporting MS Construction
		trusted, virtually instantaneous delivery on a cost-effective, convenient basis and none provide rights management and auditing through persistent, secure, digital information protection. In contrast, the present inventions provide the trustedness, confidentiality and security of a personal trusted courier on a virtually instantaneous and highly cost-effective basis. They provide techniques, systems and methods that can being to any form of electronic communications (including, but not limited to Internet and internal company electronic mail) an extremely high degree of trustedness, confidence and security approaching or exceeding that provided by a trusted personal courier. They also provide a wide variety of benefits that flow from rights management and secure chain of handling and control." ('683 5:22-40) 35. "The Virtual Distribution Environment provides comprehensive overall systems, and wide arrays of methods, techniques, structures and arrangements, that enable secure, efficient electronic commerce and rights management on the Internet and other information superhighways and on internal corporate networks such as 'Intranets'." ('683 5:41-51-56) 36. "Parties using the Virtual Distribution Environment can participate in commerce and other transactions in accordance with a persistent set of rules they electronically define." ('683 6:11-14) 37. "All of these various coordination steps can be performed nearly simultaneously, efficiently, rapidly and with an extremely high degree of trustedness based on the user of electronic containers 302 and the secure communications, authentication, notarization and archiving techniques provided in accordance with the present inventions." ('683 55:54-59) 38. "People are increasingly using secure digital containers to safely and securely store and transport digital content. One secure digital container model is the 'DigiBox™' container developed by InterTrust Technologies, Inc. of Sunnyvale, Calif. The Ginter et al. patent specification referenced above describes many characteristics of this DigiBox™ container model—a powerful, flexible, general construct that enables protected, efficient and interoperable electronic description and regulation of electronic commerce relationship of all kinds, including the secure transport, storage and rights management interface with objects and digital information within such containers." ('861 1:35-41) 39. "Briefly, DigiBox containers are tamper-resistant digital containers that can be used to package any kind of digital information such as, for example, text, graphics, executable software, audio and/or video. The rights management environment in which DigiBox™. containers are used allows commerce participants to associate rules with the digital information (content). The rights management environment also allows rules (herein including rules and parameter data controls) to be securely associated with other rights management information, such as for example, rules, audit records created during use of digital information and administrative information associated with keeping the environment working properly, including ensuring rights and any agreements among parties. The DigiBox™.. electronic container can be used to store, transport and provide a rights management interfaces to digital information, related rules and other rights management information, as well as to other objects

	Claim Term/Phrase	Evidence Supporting MS Construction
		and/or data within a distributed, rights management environment. This arrangement can be used to provide electronically enforced chain of handling and control wherein rights management persists as a container moves from one entity to another. This capability helps support a digital rights management architecture that allows content rightsholders (including any parties who have system authorized interests related to such content, such as content republishes or even governmental authorities) to securely control and manage content, events, transactions, rules and usage consequences, including any required payment and/or usage reporting. This secure control and management continues persistently, protecting rights as content is delivered to, used by, and passed among creators, distributors, repurposes, consumers, payment disagregators, and other value chain participants." ('861 1:47 - 2:12) 40. "Use of secure electronic containers to transport items provides an unprecedented degree of security, trustedness and flexibility." ('683 8:50-52) 41. "Virtual distribution environment 100 is 'virtual' because it does not require many of the physical 'things' that used to be necessary to protect rights, ensure reliable and predictable distribution, and ensure proper compensation to content creators and distributors." ('193 53:23-27) **Extrinsic:** 42. VDE: "VDE is the broad name given to a comprehensive system (algorithms, software, and hardware) that provides metering, securing, and administration tools for intellectual property. VDE stands for 'Virtual Distribution Environment.'" (VDE ROI DEVICE v1.0a, 2/9/94, IT00008570) 43. Virtual: "Pertaining to a functional unit that appears to be real, but whose functions are accomplished by other means." (IBM) 44. Environment: "1. The aggregate of external circumstances, conditions, and objects that affect the development, operation, and maintenance of a system. 2. In computer security, those factors, both internal and external, of an ADP system that help to define the risks associated with its operation." (Longley) 45. Environment: See InterTrust node: "A computer that is enabled for processing of DigiBox containers by installation of a PPE, which may be either hardware or software based. A node may include application software and/or operating system integration. The node is also termed the *environment*." (IT Glossary, 8/21/95, TD00068B, IT00032375) 46. InterTrust Commerce Architecture model: "A model that defines a general-purpose distributed architecture for secure electronic commerce and digital rights management. The InterTrust Commerce Architecture model includes four key software elements: DigiBox secure containers, InterRights Point software with associated protected database, the InterTrust Transaction Authority Framework, and the InterTrust Deployment Manager." (IT Glossary, 1997, ML00012A) 47. VDE is a system using secure computing technology to enforce a chain of handling and control representing the rights of interested parties. (IT Glossary, 3/7/95, IT00709616) 48. Virtual Distribution Environment (VDE): "A set of components that protects content and enforces rights associated with content." (IT Glossary, 3/7/95,

	Claim Term/Phrase	Evidence Supporting MS Construction
		IT00709620) 49. "Virtual Distribution Environment: or 'VDE' shall mean a system which guarantees: (I) that the content creators, publishers, and/or distributors of information receive agreed upon fees for the use of, and/or records of the use of, electronic content; and/or (ii) that stored and/or distributed information will be used only in authorized ways. More particularly, VDE relates to systems for applying controls to, and controlling and/or auditing use of, electronically stored and/or disseminated information." (License Agreement, National Semiconductor and EPR, 3/18/94, Exhibit 12 to IT 30(b)(6)) 50. See also IT0001689-96, IT0709785 (VDE on a Page), IT000202-29 (2) <u>SECURE PROCESSING ENVIRONMENT</u>: 1. "VDE allows the needs of electronic commerce participants, to be served and it can bind such participants together in a universe wide, trusted commercial network that can be secure enough to support very large amounts of commerce. VDE's security and metering secure subsystem core will be present all physical locations where VDE related contents is (a) assigned usage related control information (rules and mediating data), and/or (b) used. This core can perform security and auditing functions (including metering) that operate within a 'virtual black box,' a collection of distributed, very secure VDE related hardware instances that are interconnected by secured information exchange (for example, telecommunication) processes and distributed database means." ('193 15:14-27) 2. "Summary of Some Important Features Provided by VDE in Accordance With the Present Invention … VDE employs special purpose hardware distributed throughout some or all locations of a VDE implementation: a) said hardware controlling important elements of: content preparation (such as causing such content to be placed in a VDE content container and associating content control information with said content), content and/or electronic appliance usage auditing, content usage analysis, as well as content usage control; and b) said hardware having been designed to securely handle processing load module control activities, wherein said control processing activities may involve a sequence of required control factors" ('193 21:43-45; 22:20-31) 3. "Physical facility and user identity authentication security procedures may be used instead of hardware SPUs at certain nodes, such as at an established financial clearinghouse, where such procedures may provide sufficient security for trusted interoperability with a VDE arrangement employing hardware SPUs at user nodes." ('193 45:60-65) 4. "An important part of VDE provided by the present invention is the core secure transaction control arrangement, herein called an SPU (or SPUs), that typically must be present in each user's computer, other electronic appliance, or network. SPUs provide a trusted environment for generating decryption keys, encrypting and decrypting information, managing the secure communication of keys and other information between electronic appliances (i.e. between VDE installations and/or between plural VDE instances within a single VDE installation), securely accumulating and managing audit trail, reporting, and budget

	Claim Term/Phrase	Evidence Supporting MS Construction
		information in secure and/or non-secure non-volatile memory, maintaining a secure database of control information management instructions, and providing a secure environment for performing certain other control and administrative functions." ('193 48:66 - 49:17) 5. "A hardware SPU (rather than a software emulation) within a VDE node is necessary if a highly trusted environment for performing certain VDE activities is required." ('193 49:15-17) 6. "'Hardware' 506 also contains long-term and short-term memories to store information securely so it can't be tampered with." ('193 60:1-3) 7. "A VDE node's hardware SPU is a core component of a VDE secure subsystem and may employ some or all of an electronic appliance's primary control logic, such as a microcontroller, microcomputer or other CPU arrangement. This primary control logic may be otherwise employed for non VDE purposes such as the control of some or all of an electronic appliance's non-VDE functions. When operating in a hardware SPU mode, said primary control logic must be sufficiently secure so as to protect and conceal important VDE processes. For example, a hardware SPU may employ a host electronic appliance microcomputer operating in protected mode while performing VDE related activities, thus allowing portions of VDE processes to execute with a certain degree of security." ('193 49:33-46) 8. "As shown FIG. 6 [sic], in the preferred embodiment, an SPU 500 may be implemented as a single integrated circuit 'chip' 505 to provide a secure processing environment in which confidential and/or commercially valuable information can be safely processed, encrypted and/or decrypted." ('193 63:48-52) 9. "SPU 500 is enclosed within and protected by a 'tamper resistant security barrier' 502. Security barrier 502 separates the secure environment 503 from the rest of the world. It prevents information and processes within the secure environment 503 form being observed, interfered with and leaving except under appropriate secure conditions. Barrier 502 also controls external access to secure resources, processes and information within SPU 500. In one example, tamper resistant security barrier 502 is formed by security features such as 'encryption,' and hardware that detects tampering and/or destroys sensitive information within secure environment 503 when tampering is detected." ('193 59:48-59) 10. "SPU 500 may be surrounded by a tamper-resistant hardware security barrier 502. Part of this security barrier 502 is formed by a plastic or other package in which an SPU 'die' is encased. Because the processing occurring within, and information stored by, SPU 500 are not easily accessible to the outside world, they are relatively secure from unauthorized access and tampering. All signals cross barrier 502 through a secure, controlled path provided by BIU 530 that restricts the outside world's access to the internal components within SPU 500. The secure, controlled path resists attempts form the outside world to access secret information and resources within SPU 500." ('193 63:60 - 64:5)

	Claim Term/Phrase	Evidence Supporting MS Construction
		(3) VDE CONTROLS: See support as listed for Control (n.) , item #8, above. 1. "Limited only by the VDE control information employed by content creators, other providers, and other pathway of handling and control participants, VDE allows a 'natural' and unhindered flow of, and creation of, electronic content product models." ('193 297:25-29) 2. "Regulation is ensured by control information put in place by one or more parties." ('193 6:34-35) 3. "As a result, the present invention answers pressing, unsolved needs by offering a system that supports a standardized control environment which facilitates interoperability of electronic appliances, interoperability of content containers, and efficient creation of electronic commerce applications and models through the use of a programmable, secure electronic transactions management foundation and reusable and extensible executable components." ('193 8:62 - 9:3) 4. "Independently, securely deliverable, component based control information allows efficient interaction among control information sets supplied by different parties." ('193 10:46-50) 5. "A significant facet of the present invention's ability to broadly support electronic commerce is its ability to securely manage independently delivered VDE component objects containing control information (normally in the form of VDE objects containing one or more methods, data, or load module VDE components). This independently delivered control information can be integrated with senior and other pre-existing content control information to securely form derived control information using the negotiation mechanisms of the present invention. All requirements specified by this derived control information must be satisfied before VDE controlled content can be accessed or otherwise used. This means that, for example, all load modules and any mediating data which are listed by the derived control information as required must be available and securely perform their required function." ('193 10:66 - 11:14) 6. "Content control information governs content usage according to criteria set by holders of rights to an object's contents and/or according to parties who otherwise have rights associated with distributing such content (such as governments, financial credit providers, and users)." ('193 15:46-48) 7. "In part, security is enhanced by object methods employed by the present invention because the encryption schemes used to protect an object can efficiently be further used to protect the associated content control information (software control information and relevant data) from modification." ('193 15:51-55) 8. "Summary of Some Important Features Provided by VDE in Accordance With the Present Invention … Content users, such as end-user customers using commercially distributed content (games, information resources, software programs, etc.), can define, if allowed by senior control information, budgets, and/or other control information, to manage their own internal use of content." ('193 21:43-45; 29:3-8) 9. "Summary of Some Important Features Provided by VDE in Accordance With

	Claim Term/Phrase	Evidence Supporting MS Construction
		the Present Invention.... support the separation of fundamental transaction control processes through the use of event (triggered) based method control mechanisms. These event methods trigger one or more other VDE methods (which are available to a secure VDE sub-system) and are used to carry out VDE managed transaction related processing. These triggered methods include independently (separably) and securely processable component billing management methods, budgeting management methods, metering management methods, and related auditing management processes. As a result of this feature of the present invention, independent triggering of metering, auditing, billing, and budgeting methods, the present invention is able to efficiently, concurrently support multiple financial currencies (e.g. dollars, marks, yen) and content related budgets, and/or billing increments as well as very flexible content distribution models." ('193 21:43-45; 42:21-38) 10. "Summary of Some Important Features Provided by VDE in Accordance With the Present Invention....support, complete, modular separation of the control structures related to (1) content event triggering, (2) auditing, (3) budgeting (including specifying no right of use or unlimited right of use), (4) billing, and (5) user identity (VDE installation, client name, department, network, and/or user, etc.). The independence of these VDE control structures provides a flexible system which allows plural relationships between two or more of these structures, for example, the ability to associate a financial budget with different event trigger structures (that are put in place to enable controlling content based on its logical portions). Without such separation between these basic VDE capabilities, it would be more difficult to efficiently maintain separate metering, budgeting, identification, and/or billing activities which involve the same, differing (including overlapping), or entirely different, portions of content for metering, billing, budgeting, and user identification, for example, paying fees associated with usage of content, performing home banking, managing advertising services, etc. VDE modular separation of these basic capabilities supports the programming of plural, 'arbitrary' relationships between one or differing content portions (and/or portion units) and budgeting, auditing, and/or billing control information." ('193 21:43-45; 42:39-63) 11. "The virtual distribution environment 100 prevents use of protected information except as permitted by the 'rules and controls' (control information). For example, the 'rules and controls' shown in FIG. 2 may grant specific individuals or classes of content users 112 'permission' to use certain content. They may specify what kinds of content usage are permitted, and what kinds are not. They may specify how content usage is to be paid for and how much it costs. As another example, 'rules and controls' may require content usage information to be reported back to the distributor 106 and/or content creator 102." ('193 56:26-35) 12. "ROS VDE functions 604 may be based on segmented, independently loadable executable 'component assemblies' 690. These component assemblies 690 are independently securely deliverable. The component assemblies 690 provided by the preferred embodiment comprise code and data elements that are themselves independently deliverable.... These component assemblies 690 are the basic

	Claim Term/Phrase	Evidence Supporting MS Construction
		functional unit provided by ROS 602. The component assemblies 690 are executed to perform operating system or application tasks. Thus, some component assemblies 690 may be considered to be part of the ROS operating system 602, while other component assemblies may be considered to be 'applications' that run under the support of the operating system." ('193 83:12-29) 13. "As mentioned above, ROS 602 provides several layers of security to ensure the security of component assemblies 690. One important security layer involves ensuring that certain component assemblies 690 are formed, loaded and executed only in secure execution space such as provided within an SPU 500." ('193 87:33-38) 14. "Methods 1000 perform the basic function of defining what users (including, where appropriate, distributions, client administration, etc.), can and cannot do with an object 300." ('193 128:30-33) 15. "Container 152 in this example further includes an electronic control set 188 describing conditions under which the power may be exercised. Controls 188 define the power(s) granted to each of the participants – including (in this example) conditions or limitations for exercising these powers. Controls 188 may provide the same powers and/or conditions of use for each participant, or they may provide different powers and/or conditions of use for each participant." ('712 220:1-8) 16. "…content creators and rights owners can register permissions with the rights and permissions clearinghouses 400 in the form of electronic 'control sets.' These permissions can specify what consumers can and can't do with digital properties, under what conditions the permissions can be exercised and the consequences of exercising the permissions." ('712 72:2-7) 17. "This 'channel 0' 'open channel' task may then issue a series of requests to secure database manager 566 to obtain the 'blueprint' for constructing one or more component assemblies 690 to be associated with channel 594 (block 1127). In the preferred embodiment, this 'blueprint' may comprise a PERC 808 and/or URT 464." ('193 112:46-51) (4) <u>VDE Secure Container</u>: See support as listed for Secure Container, item #20, above. **Intrinsic:** 1. "In part, security is enhanced by object methods employed by the present invention because the encryption schemes used to protect an object can efficiently be further used to protect the associated content control information (software control information and relevant data) from modification." ('193 15:51-55) 2. "FIG. 5A shows how the virtual distribution environment 100, in a preferred embodiment, may package information elements (content) into a 'container' 302 so the information can't be accessed except as provided by its 'rules and controls.' Normally, the container 302 is electronic rather than physical. Electronic container 302 in one example comprises 'digital' information having a well defined structure. Container 302 and its contents can be called an 'object

	Claim Term/Phrase	Evidence Supporting MS Construction
		300.'" ('193 58:39-46) 3. "Moreover, when any new VDE object 300 arrives at an electronic appliance 600, the electronic appliance must 'register' the object within object registry 450 so that it can be accessed." ('193 153:56-59) 4. "Even if the object is stored locally to the VDE node, it may be stored as a secure or protected object so that it is not directly accessible to a calling process. ACCESS method 2000 establishes the connections, routings, and security requisites needed to access the object." ('193 192:14-19) 5. "ACCESS method 2000 reads the ACCESS method MDE from the secure database, reads it in accordance with the ACCESS method DTD, and loads encrypted content source and routing information based on the MDE (blocks 2010, 2012). This source and routing information specifies the location of the encrypted content. ACCESS method 2000 then determines whether a connection to the content is available (decision block 2014). This 'connection' could be, for example, an on-line connection to a remote site, a real-time information feed, or a path to a secure/protected resource, for example. If the connection to the content is not currently available ('No' exit of decision block 2014), then ACCESS method 2000 takes steps to open the connection (block 2016). If the connection fails (e.g., because the user is not authorized to access a protected secure resource), then the ACCESS method 2000 returns with a failure indication (termination point 2018)." ('193 192:36-52) 6. "It also employs a software object architecture for VDE content containers that carries protected content and may also carry both freely available information (e.g., summary, table of contents) and secured content control information which ensures the performance of control information." ('193 15:41-46) 7. "In this example, creator 102 may employ one or more application software programs and one or more VDE secure subsystems to place unencrypted content into VDE protected form (i.e., into one or more VDE content containers)." ('193 315:53-56) 8. "The Ginter et al. patent specification referenced above describes many characteristics of this DigiBox™ container model, a powerful, flexible, general construct that enables protected, efficient and interoperable electronic description and regulation of electronic commerce relationships of all kinds..." ('861 1:39-44) 9. "The node and container model described above and in the Ginter et al. patent specification (along with similar other DigiBox/VDE (Virtual Distribution Environment) models) has nearly limitless flexibility." ('861 2:37-40) 10. "Therefore, the container creation and usage tools must themselves be secure in the sense that they must protect certain details about the container design. This additional security requirement can make it even more difficult to make containers easy to use and to provide interoperability." ('861 4:59-64) 11. "FIG. 88 illustrates secure electronic container 302 as an attaché handcuffed to the secure delivery person's wrist. Once again, container is shown as a physical thing for purposes of illustrations only --in the example it is preferably electronic rather than physical, and comprises digital information having a well-defined structure (see FIG. 5A). Special mathematical techniques known as

	Claim Term/Phrase	Evidence Supporting MS Construction
		'cryptography' can be used to make electronic container 302 secure so that only intended recipient 4056 can open the container and access the electronic document (or other items) 4054 it contains." ('683 15:61 - 16:14) 12. "Appliance 600B may deliver the digital copy of item 4054 within a container 302 and/or protect the item with seals. Electronic fingerprints, watermarks and/or other visible and/or hidden markings to provide a 'virtual container'or some of the security or other characteristics of a container (for example, the ability to associate electronic controls with the item). ('683 18:49-56) 13. "For example, defendant's attorney 5052 can specify one container 302 for opening by his co-counsel, client or client in-house counsel, and program another container 302 for opening only by opposing (plaintiff's) counsel 5050. Because of the unique trustedness features provided by system 4050, the defendant's attorney 5052 can have a high degree of trust and confidence that only the authorized parties will be able to open the respective containers and access the information they contain." ('683 56:17-25) 14. "The 'container' concept is a convenient metaphor used to give a name to the collection of elements required to make use of content or to perform an administrative-type activity." ('193 127:30-32) 15. "The virtual distribution environment 100, in a preferred embodiment, may package information elements (content) into a 'container' 302 so the information can't be accessed except as provided by its 'rules and controls.'" ('193 58:39-43) 16. "VDE 100 provides a media independent container model for encapsulating content." ('193 127:2-3) 17. "The electronic form of a document is stored as a VDE container (object) associated with the specific client and/or case. The VDE container mechanism supports a hierarchical ordering scheme for organizing files and other information with a container; this mechanism may be used to organize the electronic copies of the documents within a container, A VDE container is associated with specific access control information and rights that are described in one or more permissions control information sets (PERCs) associated with that container. In this example, only those members of the law firm who possess a VDE instance, an appropriate PERC, and the VDE object that contains the desired document, may use the document." ('193 274:52-64) 18. "The situation is no better for processing documents within the context of ordinary computer and network systems. Although said systems can enforce access control information based on user identity, and can provide auditing mechanism for tracking accesses to files, these are low-level mechanisms that do not permit tracking or controlling the flow of content. In such systems, because document content can be freely copied and manipulated, it is not possible to determine where documents content has gone, or where it came from." ('193 281:27-35) 19. "Secure containers 302 may be used to encapsulate the video and audio being exchanged between electronic kiosk appliances 600, 600' to maintain confidentiality and ensure a high degree of trustedness." ('682 52: 61-64) 20. "[C]ontainer 152 can only be opened within a secure protected processing

	Claim Term/Phrase	Evidence Supporting MS Construction
		environment 154 that is part of the virtual distribution environment described in the above-referenced Ginter et al. patent disclosure ...." ('712 168:22-25) 21. "The present invention provides a new kind of 'virtual distribution environment' (called 'VDE' in this document) that secures, administers, and audits electronic information use. VDE also features fundamentally important capabilities for managing content that travels 'across' the 'information highway.'" ('193 2:24-28) 22. "The present invention truly achieves a content control and auditing architecture that can be configured to most any commercial distribution embodiment." ('193 261:12-15) 23. "The inability of conventional products to be shaped to the needs of electronic information providers and users is sharply in contrast to the present invention. Despite the attention devoted by a cross-section of America's largest telecommunications, computer, entertainment and information provider companies to some of the problems addressed by the present invention, only the present invention provides commercially secure, effective solutions for configurable, general purpose electronic commerce transaction/distribution control systems." ('193 2:13-22) 24. "The configurability provided by the present invention is particularly critical for supporting electronic commerce, that is enabling businesses to create relationships and evolve strategies that offer competitive value. Electronic commerce tools that are not inherently configurable and interoperable will ultimately fail to produce products (and services) that meet both basic requirements and evolving needs of most commerce applications." ('193 16:41-48) 25. "VDE also extends usage control information to an arbitrary granular level (as opposed to a file based level provided by traditional operating systems) ...." ('193 275:8-11) 26. "Summary of Some Important Features Provided by VDE in Accordance With the Present Invention: ...." ('193 21:43-45) 27. "A significant facet of the present invention's ability to broadly support electronic commerce is its ability to securely manage independently delivered VDE component objects containing control information ..." ('193 10:66 - 11:2) 28. "Some of the key factors contributing to the configurability intrinsic to the present invention include: ...." ('193 16:66-67) 29. "The scalable transaction management/auditing technology of the present invention will result in more efficient and reliable interoperability ...." ('193 34:9-11) 30. "The present invention answers pressing, unsolved needs by offering a system that supports a standardized control environment which facilitates interoperability of electronic appliances, interoperability of content containers, and efficient creation of electronic commerce applications and models through the use of a programmable, secure electronic transactions management foundation and reusable and extensible executable components." ('193 8:63 - 9:3)

	Claim Term/Phrase	Evidence Supporting MS Construction
		31. "The design of the VDE foundation, VDE load modules, and VDE containers, are important features that enable the VDE node operating environment to be compatible with a very broad range of electronic appliances." ('193 34:26-30) 32. "The ability to optionally incorporate different methods 1000 with each object is important to making VDE 100 highly configurable." ('193 128:28-30) 33. "An important feature of VDE is that it can be used to assure the administration of, and adequacy of security and rights protection for, electronic agreements implemented through the use of the present invention." ('193 46:51-54) 34. "In this example, both the address request 602 and the responsive information 604 are contained within secure electronic containers 152 in order to maintain the confidentiality and integrity of the requests and responses. In this way, for example, outside eavesdroppers cannot tell who sender 95(1) wants to communicate with or what information he or she needs to perform communications with or what information he or she needs to perform the communications – and the directory responses cannot be 'spoofed' to direct the requested message to another location." ('712 12:15-22) 35. "On the other hand, if the information to be exchanged has already been secured and/or is available without authentication (e.g., certain catalog information, containers that have already been encrypted and do not require special handling, etc.), the 'weaker' form of login/password may be used." ('193 290:57-62) 36. "VDE provides means to securely combine content provided at different times, by differing sources, and/or representing different content types. These types, timings, and/or different sources of content can be employed to form a complex array of content within a VDE content container objects, each containing different content whose usage can be controlled, at least in part, by its own container's set of VDE content control information." ('193 297:35-45) 37. "Although methods 1000 can have virtually unlimited variety and some may even be user-defined, certain basic 'use' type methods are preferably used in the preferred embodiment to control most of the more fundamental object manipulation and other functions provided by VDE 100. For example, the following high level methods would typically be provided for object manipulation; OPEN method, READ method, WRITE method, CLOSE method. An OPEN method is used to control opening a container so its content may be accessed. A READ method is used to control access to contents in a container. A WRITE method is used to control the insertion of contents into a container. A CLOSE method is used to close a container that has been opened." ('193 183:12-29) 38. "DESTROY method 2180 removes the ability of a user to use an object by destroying the URT the user requires to access the object. In the preferred embodiment, ... DESTROY method 2180 may than *[sic]* call a WRITE and/or ACCESS method to write information which will corrupt (and thus destroy) the header and/or other important parts of the object (block 2186). DESTROY method 2180 may then mark one or more of the control structures (e.g., the URT) as damaged by writing appropriate information to control structure (blocks 2188, 2190)." ('193 198:41-45) 39. "PANIC method 2200 may prevent the user from further accessing the object

	Claim Term/Phrase	Evidence Supporting MS Construction
		currently being accessed by, for example, destroying the channel being used to access the object and marking one or more of the control structures (e.g., the URT) associated with the user and object as damaged.(blocks 2206, and 2208-2210, respectively). Because the control structure is damaged, the VDE node will need to contact an administrator to obtain a valid control structure(s) before the user may access the same object again." ('193 198:60 - 199:2) 40. "EXTRACT method 2080 is used to copy or remove content from an object and place it into a new object. In the preferred embodiment, the EXTRACT method 2080 does not involve any release of content, but rather simply takes content from one container and places it into another container, both of which may be secure. Extraction of content differs from release in that the content is never exposed outside a secure container." ('193 194:13-20) 41. "Use of secure electronic containers to transport items provides an unprecedented degree of security, trustedness and flexibility." ('683 8:50-52) 42. "Electronic delivery person 4060 can deliver the electronic version of item 4054 within secure container attaché case 302 from personal computer 4116' to another personal computer 4116 operated by recipient 4056." ('683 20:27-30) 43. "Because these transactions are conducted using VDE and VDE secure containers, those observing the communications learn no more than the fact that the parties are communicating." ('712 310:1-3) 44. "VDE in one example provides a 'virtual silicon container' ('virtual black box') in that several different instances of SPU 500 may securely communicate together to provide an overall secure hardware environment that 'virtually' exists at multiple locations and multiple electronic appliances 600. FIG. 87 shows one model 3600 of a virtual silicon container. This virtual container model 3600 includes a content creator 102, a content distributor 106, one or more content redistributors 106a, one or more client administrators 700, one or more client users 3602, and one or more clearinghouses 116. Each of these various VDE participants has an electronic appliance 600 including a protected processing environment 655 that may comprise, at least in part, a silicon-based semiconductor hardware element secure processing unit 500. The various SOUs 500 each encapsulate a part of the virtual distribution environment, and thus, together form the virtual silicon container 3600." ('193 317:58 - 318:8) 45. "Uses tools to transform digital information(such as electronic books, databases, computer software and movies) into protected digital packages called 'objects.' Only those consumers (or other along the chain of possession such as redistributor) who receive permission from a distributor 106 can open these packages. VDE packaged content can be constrained by 'rules and control information.'" ('193 254:18-25) 46. "To open VDE package and make use of its content, and end-user must have permission." ('193 254:45-46) 47. "Place unencrypted content into VDE protected form (i.e., into one or more VDE content containers)." ('193 315:55-56) (5) <u>NON-CIRCUMVENTABLE</u>: **Intrinsic**:

	Claim Term/Phrase	Evidence Supporting MS Construction
		1. "VDE can protect a collection of rights belonging to various parties having in rights in, or to, electronic information. This information may be at one location or dispersed across (and/or moving between) multiple locations. The information may pass through a 'chain' of distributors and a 'chain' of users. Usage information may also be reported through one or more 'chains' of parties. In general, VDE enables parties that (a) have rights in electronic information, and/or (b) act as direct or indirect agents for parties who have rights in electronic information, to ensure that the moving, accessing, modifying, or otherwise using of information can be securely controlled by rules regarding how, when, where, and by whom such activities can be performed." ('193 6:18-31) 2. "All requirements specified by this derived control information must be satisfied before VDE controlled content can be accessed or otherwise used. ('193 11:8-11) 3. "VDE provides important mechanisms for both enforcing commercial agreements and enabling the protection of privacy rights. VDE can securely deliver information from one party to another concerning the use of commercially distributed electronic content. Even if parties are separated by several 'steps' in a chain (pathway) of handling for such content usage information, such information is protected by VDE through encryption and/or other secure processing. Because of that protection, the accuracy of such information is guaranteed by VDE, and the information can be trusted by all parties to whom it is delivered." ('193 14:29-39) 4. "VDE ensures that certain prerequisites necessary for a given transaction to occur are met. This includes the secure execution of any required load modules and the availability of any required, associated data." ('193 20:27-30) 5. "Required methods (methods listed as required for property and/or appliance use) must be available as specified if VDE controlled content (such as intellectual property distributed within a VDE content container) is to be used." ('193 43:37-41) 6. "Since all secure communications are at least in part encrypted and the processing inside the secure subsystem is concealed from outside observation and interference, the present invention ensures that content control information can be enforced." ('193 46:4-8) 7. "This control information can determine, for example: (1) How and/or to whom electronic content can be provided, for example, how an electronic property can be distributed; (2) How one or more objects and/or properties, or portions of an object or property, can be directly used, such as decrypted, displayed, printed, etc; …." ('193 46:17-24) 8. "'Hardware' 506 also contains long-term and short-term memories to store information securely so it can't be tampered with." ('193 60:1-3) 9. "A feature of VDE provided by the present invention is that certain one or more methods can be specified as required in order for a VDE installation and/or user to be able to use certain and/or all content." ('193 43:47-50) 10. "The virtual distribution environment 100 prevents use of protected information

	Claim Term/Phrase	Evidence Supporting MS Construction
		except as permitted by the 'rules and controls' (control information)." ('193 56:26-28) 11. "As mentioned above, virtual distribution environment 100 'associates' content with corresponding 'rules and controls,' and prevents the content from being used or accessed unless a set of corresponding 'rules and controls' is available. The distributor 106 doesn't need to deliver content to control the content's distribution. The preferred embodiment can securely protect content by protecting corresponding, usage enabling 'rules and controls' against unauthorized distribution and use." ('193 57:18-26) 12. "Since no one can use or access protected content without 'permission' from corresponding 'rules and controls,' the distributor 106 can control use of content that has already been (or will in the future be) delivered." ('193 57:30-33) 13. "SPU 500 is enclosed within and protected by a 'tamper resistant security barrier' 502. Security barrier 502 separates the secure environment 503 from the rest of the world. It prevents information and processes within the secure environment 503 from being observed, interfered with and leaving except under appropriate secure conditions. Barrier 502 also controls external access to secure resources, processes and information within SPU 500." ('193 59:48-55) 14. "Provides non-repudiation of use and may record specific forms of use such as viewing, editing, extracting, copying, redistributing (including to what one or more parties), and/or saving." ('683 6:46-48) 15. "In general, VDE enables parties that (a) have rights in electronic information, and/or (b) act as direct or indirect agents for parties who have rights in electronic information, to ensure that the moving, accessing, modifying, or otherwise using of information can be securely controlled by rules regarding how, when, where, and by whom such activities can be performed." ('193 6:24-30) 16. "To securely control access and other use, including distribution of records, documents, and notes associated with the case" ('193 274:34-36) 17. "Thus wrapped, a VDE object may be distributed to the recipient without fear of unauthorized access and/or other use." ('193 277:16-17) 18. "These appliances typically include a secure subsystem that can enable control of content use such as displaying, encrypting, decrypting, printing, copying, saving, extracting, embedding, distributing, auditing usage, etc." ('193 9:24-27) 19. "VDE provides a secure, distributed electronic transaction management system for controlling the distribution and/or other usage of electronically provided and/or stored information." ('193 9:36-39) 20. "The control set 404 might permit publisher 168 to add his own additional controls that allow consumer 95 to read the work 166 an unlimited number of time but prevent the consumer from copying or redistributing the work." (712 258: 8-11) 21. "The doctor 5000 may then send container 301(1) to a trusted go-between 4700. … For example, the trusted go-between 4700 in one example has no access to the content of the container 302(1), but does have a record of a seal of

	Claim Term/Phrase	Evidence Supporting MS Construction
		the contents." ('683 53:40-57) 22. "FIG. 116 shows example steps that may be performed by PPE 650 in response to an 'open' or 'view' event. In this example, PPE 650 may - - upon allowing recipient 4056 to actually interact with the item 4054—...PPE 650 may then release the image 4068I and/or the data 4068D to the application running on electronic appliance 600—electronic fingerprinting or watermarking the released content if appropriate (FIG. 116, block 4625C). ('683 42:38-52) 23. "FIG. 5A shows how the virtual distribution environment 100, in a preferred embodiment, may package information elements (content) into a 'container' 302 so the information can't be accessed except as provided by its 'rules and controls.'" ('193 58:39-43) (6) PEER TO PEER: **Intrinsic:** 1. "Each VDE participant in a VDE pathway of content control information may set methods for some or all of the content in a VDE container, so long as such control information does not conflict with senior control information already in place with respect to: (1) certain or all VDE managed content, (2) certain one or more VDE users and/or groupings of users, (3) certain one or more VDE nodes and/or groupings of nodes, and/or (4) certain one or more VDE applications and/or arrangements." ('193 44:6-17) 2. "All participants of VDE 100 have the innate ability to participate in any role." ('193 256:50-51) 3. "Any VDE user 112 may assign the right to process information or perform services on their behalf to the extent allowed by senior control information." ('193 257:17-20) 4. "PERC and URT structures provide a mechanism that may be used to provide precise electronic representation of rights and the controls associated with those rights. VDE thus provides a 'vocabulary' and mechanism by which users and creators may specify their desires." ('193 245:11-15) (7) COMPREHENSIVE RANGE OF FUNCTIONS: **Intrinsic:** 1. "VDE provides comprehensive and configurable transaction management, metering and monitoring technology." ('193 3:34-35) 2. "VDE may be combined with, or integrated into, many separate computers and/or other electronic appliances. These appliances typically include a secure subsystem that can enable control of content use such as displaying, encrypting, decrypting, printing, copying, saving, extracting, embedding, distributing, auditing usage, etc. The secure subsystem in the preferred embodiment comprises one or more 'protected processing environments', one or more secure databases, and secure 'component assemblies' and other items and processes that need to be kept secured. VDE can, for example, securely control electronic currency, payments, and/or credit management (including electronic credit and/or currency receipt, disbursement, encumbering, and/or allocation) using such a 'secure subsystem.'" ('193 9:22-35)

	Claim Term/Phrase	Evidence Supporting MS Construction
		3. "In addition VDE: (a) is very configurable, modifiable, and re-usable; (b) supports a wide range of useful capabilities that may be combined in different ways to accommodate most potential applications; (c) operates on a wide variety of electronic appliances ranging from hand-held inexpensive devices to large mainframe computers; (d) is able to ensure the various rights of a number of different parties, and a number of different rights protection schemes, simultaneously; (e) is able to preserve the rights of parties through a series of transactions that may occur at different times and different locations; (f) is able to flexibly accommodate different ways of securely delivering information and reporting usage; and (g) provides for electronic analogues to 'real' money and credit, including anonymous electronic cash, to pay for products and services and to support personal (including home) banking and other financial activities." ('193 4:57 - 5:10) 4. "[VDE] can provide efficient, reusable, modifiable, and consistent means for secure electronic content: distribution, usage control, usage payment, usage auditing, and usage reporting." ('193 8:26-29) 5. "VDE offers an architecture that avoids reflecting specific distribution biases, administrative and control perspectives, and content types. Instead, VDE provides a broad-spectrum, fundamentally configurable and portable, electronic transaction control, distributing, usage, auditing, reporting, and payment operating environment." ('193 8:53-58) 6. "The present invention allows content providers and users to formulate their transaction environment to accommodate: (1) desired content models, content control models, and content usage information pathways, (2) a complete range of electronic media and distribution means, (3) a broad range of pricing, payment, and auditing strategies, (4) very flexible privacy and/or reporting models, (5) practical and effective security architectures, and (6) other administrative procedures that together with steps (1) through (5) can enable most 'real world' electronic commerce and data security models, including models unique to the electronic world." ('193 10:11-23) 7. "Because of the breadth of issues resolved by the present invention, it can provide the emerging 'electronic highway' with a single transaction/distribution control system that can, for a very broad range of commercial and data security models, ensure against unauthorized use of confidential and/or proprietary information and commercial electronic transactions." ('193 17:22-28) 8. "A feature of the present invention provides for payment means supporting flexible electronic currency and credit mechanisms, including the ability to securely maintain audit trails reflecting information related to use of such currency or credit.' ('193 33:58-63) 9. "The end-to-end nature of VDE applications, in which content 108 flows in one

	Claim Term/Phrase	Evidence Supporting MS Construction
		direction, generating reports and bills 118 in the other, makes it possible to perform 'back-end' consistency checks." ('193 223:17-20) 10. "By way of non-exhaustive summary, these present inventions provide a highly secure and trusted item delivery and agreement execution services providing the following features and functions: Trustedness and security approaching or exceeding that of a personal trusted courier. Instant or nearly instant delivery. Optional delayed delivery ("store and forward"). Broadcasting to multiple parties. Highly cost effective. Trusted validation of item contents and delivery. Value Added Delivery and other features selectable by the sender and/or recipient. Provides electronic transmission trusted auditing and validating. Allows people to communicate quickly, securely, and confidentially. Communications can later be proved through reliable evidence of the communications transaction--providing non-repudiatable, certain, admissible proof that a particular communications transaction occurred. Provides non-repudiation of use and may record specific forms of use such as viewing, editing, extracting, copying, redistributing (including to what one or more parties), and/or saving. Supports persistent rights and rules based document workflow management at recipient sites. System may operate on the Internet, on internal organization and/or corporate networks ("intranets" irrespective of whether they use or offer Internet services internally), private data networks and/or using any other form of electronic communications. System may operate in non-networked and/or intermittently networked environments. Legal contract execution can be performed in real time, with or without face to face or ear-to-ear personal interactions (such as audiovisual teleconferencing, automated electronic negotiations, or any combination of such interactions) for any number of distributed individuals and/or organizations using any mixture of interactions. The items delivered and/or processed may be any 'object' in digital format, including, but not limited to, objects containing or representing data types such as text, images, video, linear motion pictures in digital format, sound recordings and other audio information, computer software, smart agents, multimedia, and/or objects any combination of two or more data types contained within or representing a single compound object. Content (executables for example) delivered with proof of delivery and/or execution or other use. Secure electronic containers can be delivered. The containers can maintain control, audit, receipt and other information and protection securely and persistently in association with one or more items.

	Claim Term/Phrase	Evidence Supporting MS Construction
		Trustedness provides non-repudiation for legal and other transactions. Can handle and send any digital information (for example, analog or digital information representing text, graphics, movies, animation, images, video, digital linear motion pictures, sound and sound recordings, still images, software computer programs or program fragments, executables, data, and including multiple, independent pieces of text; sound clips, software for interpreting and presenting other elements of content, and anything else that is electronically representable). Provides automatic electronic mechanisms that associate transactions automatically with other transactions. System can automatically insert or embed a variety of visible or invisible 'signatures' such as images of handwritten signatures, seals, and electronic 'fingerprints' indicating who has 'touched' (used or other interacted with in any monitorable manner) the item. System can affix visible seals on printed items such as documents for use both in encoding receipt and other receipt and/or usage related information and for establishing a visible presence and impact regarding the authenticity, and ease of checking the authenticity, of the item. Seals can indicate who originated, sent, received, previously received and redistributed, electronically view, and/or printed and/or otherwise used the item. Seals can encode digital signatures and validation information providing time, location, send and/or other information and/or providing means for item authentication and integrity check. Scanning and decoding of item seals can provide authenticity/integrity check of entire item(s) or part of an item (e.g., based on number of words, format, layout, image--picture and/or test--composition, etc.). Seals can be used to automatically associate electronic control sets for use in further item handling. System can hide additional information within the item using 'stenanography' for later retrieval and analysis. Steganography can be used to encode electronic fingerprints and/or other information into an item to prevent deletion. Multiple stenanographic storage of the same fingerprint information may be employed reflecting 'more' public and 'less' public modes so that a less restricted steganographic mode (different encryption algorithm, keys, and/or embedding techniques) can be used to assist easy recognition by an authorized party and a more private (confidential) mode may be readable by only a few parties (or only one party) and comprise of the less restricted mode may not affect the security of the more private mode. Items such as documents can be electronically, optically scanned at the sender's end--and printed out in original, printed form at the recipient's end. Document handlers and processors can integrate document scanning and delivery. Can be directly integrated into enterprise and Internet (and similar network) wide document workflow systems and applications. Secure, tamper-resistant electronic appliance, which may employ VDE SPUs,

	Claim Term/Phrase	Evidence Supporting MS Construction
		used to handle items at both sender and recipient ends. 'Original' item(s) can automatically be destroyed at the sender's end and reconstituted at the recipient's end to prevent two originals from existing simultaneously. Secure, non-repudiable authentication of the identification of a recipient before delivery using any number of different authentication techniques including but not limited to biometric techniques (such as palm print scan, signature scan, voice scan, retina scan, iris scan, biometric fingerprint and/or handprint scan, and/or face profile) and/or presentation of a secure identity 'token.' Non-repudiation provided through secure authentication used to condition events (e.g., a signature is affixed onto a document only if the system securely authenticates the sender and her intention to agree to its contents). Variety of return receipt options including but not limited to a receipt indicating who opened a document, when, where, and the disposition of the document (stored, redistributed, copied, etc.). These receipts can later be used in legal proceedings and/or other contexts to prove item delivery, receipt and/or knowledge. Audit, receipt, and other information can be delivered independently from item delivery, and become securely associated with an item within a protected processing environment. Secure electronic controls can specify how an item is to be processed or otherwise handled (e.g., document can't be modified, can be distributed only to specified persons, collections of persons, organizations, can be edited only by certain persons and/or in certain manners, can only be viewed and will be 'destroyed' after a certain elapse of time or real time or after a certain number of handlings, etc.) Persistent secure electronic controls can continue to supervise item workflow even after it has been received and 'read.' Use of secure electronic containers to transport items provides an unprecedented degree of security, trustedness and flexibility. Secure controls can be used in conjunction with digital electronic certificates certifying as to identity, class (age, organization membership, jurisdiction, etc.) of the sender and/or receiver and/or user of communicated information. Efficiently handles payment and electronic addressing arrangements through use of support and administrative services such as a Distributed Commerce Utility as more fully described in the copending Shear, et al. application. Compatible with use of smart cards, including, for example, VDE enabled smart cards, for secure personal identification and/or for payment. Transactions may be one or more component transactions of any distributed chain of handling and control process including Electronic Data Interchange (EDI) system, electronic trading system, document workflow sequence, and banking and other financial communication sequences, etc." ('683 6:18 - 9:4) 11. "Content providers and distributors have devised a number of limited function rights protection mechanisms to protect their rights. Authorization passwords and protocols, license servers, 'lock/unlock' distribution methods, and non-electronic contractual limitations imposed on users of shrink-wrapped software

	Claim Term/Phrase	Evidence Supporting MS Construction
		are a few of the more prevalent content protection schemes. In a commercial context, these efforts are inefficient and limited solutions." ('193 3:1-9) (8) <u>USER-CONFIGURABLE</u>: **Intrinsic:** 1. "The inability of conventional products to be shaped to the needs of electronic information providers and users is sharply in contrast to the present invention. Despite the attention devoted by a cross-section of America's largest telecommunications, computer, entertainment and information provider companies to some of the problems addressed by the present invention, only the present invention provides commercially secure, effective solutions for configurable, general purpose electronic commerce transaction/distribution control systems." ('193 2:13-22) 2. "The features of VDE allow it to function as the first trusted electronic information control environment that can conform to, and support, the bulk of conventional electronic commerce and data security requirements. In particular, VDE enables the participants in a business value chain model to create an electronic version of traditional business agreement terms and conditions and further enables these participants to shape and evolve their electronic commerce models as they believe appropriate to their business requirements." ('193 8:43-52) 3. "An objective of VDE is supporting a transaction/distribution control standard. Development of such a standard has many obstacles, given the security requirements and related hardware and communications issues, widely differing environments, information types, types of information usage, business and/or data security goals, varieties of participants, and properties of delivered information. A significant feature of VDE accommodates the many, varying distribution and other transaction variables by, in part, decomposing electronic commerce and data security functions into generalized capability modules executable within a secure hardware SPU and/or corresponding software subsystem and further allowing extensive flexibility in assembling, modifying, and/or replacing, such modules (e.g. load modules and/or methods) in applications run on a VDE installation foundation. This configurability and reconfigurability allows electronic commerce and data security participants to reflect their priorities and requirements through a process of iteratively shaping an evolving extended electronic agreement (electronic control model)." ('193 15:66 - 16:18) 4. "Some of the key factors contributing to the configurability intrinsic to the present invention include: (a) integration into the fundamental control environment of a broad range of electronic appliances through portable API and programming language tools that efficiently support merging of control and auditing capabilities in nearly any electronic appliance environment while maintaining overall system security; (b) modular data structures; (c) generic content model;

	Claim Term/Phrase	Evidence Supporting MS Construction
		(d) general modularity and independence of foundation architectural components; (e) modular security structures; (f) variable length and multiple branching chains of control; and (g) independent, modular control structures in the form of executable load modules that can be maintained in one or more libraries, and assembled into control methods and models, and where such model control schemes can 'evolve' as control information passes through the VDE installations of participants of a pathway of VDE content control information handling." ('193 16:66 - 17:21) 5. "Summary of Some Important Features Provided by VDE in Accordance With the Present Invention: ... VDE employs a variety of capabilities that serve as a foundation for a general purpose, sufficiently secure distributed electronic commerce solution. VDE enables an electronic commerce marketplace that supports divergent, competitive business partnerships, agreements, and evolving overall business models. For example, ... provide mechanisms that allow control information to 'evolve' and be modified according, at least in part, to independently, securely delivered further control information.... Handlers in a pathway of handling of content control information, to the extent each is authorized, can establish, modify, and/or contribute to, permission, auditing, payment, and reporting control information related to controlling, analyzing, paying for, and/or reporting usage of, electronic content and/or appliances (for example, as related to usage of VDE controlled property content)." ('193 21:43-46; 29:21-41) 6. "Summary of Some Important Features Provided by VDE in Accordance With the Present Invention: ... VDE employs a variety of capabilities that serve as a foundation for a general purpose, sufficiently secure distributed electronic commerce solution. VDE enables an electronic commerce marketplace that supports divergent, competitive business partnerships, agreements, and evolving overall business models. For example, ... enable a user to securely extract, through the use of the secure subsystem at the user's VDE installation, at least a portion of the content included within a VDE content container to produce a new, secure object (content container), such that the extracted information is maintained in a continually secure manner through the extraction process." ('193 21:43-46; 31:66 - 32:5) 7. "As with the content control information for most VDE managed content, features of the present invention allows [sic] the content's control information to: (a) 'evolve,' for example, the extractor of content may add new control methods and/or modify control parameter data, such as VDE application compliant methods, to the extent allowed by the content's in-place control information. ... (b) allow a user to combine additional content with at least a portion of said extracted content, ... (c) allow a user to securely edit at least a portion of said content while maintaining said content in a secure form within said VDE content container; ... (d) append extracted content to a pre-existing VDE content container object and attach associated control information ... (e) preserve VDE control over one or more portions of extracted content after

	Claim Term/Phrase	Evidence Supporting MS Construction
		various forms of usage of said portions … Generally, the extraction features of the present invention allow users to aggregate and/or disseminate and/or otherwise use protected electronic content information extracted from content container sources while maintaining secure VDE capabilities thus preserving the rights of providers in said content information after various content usage processes." ('193 32:27 - 33:4) 8. "The secure component based architecture of ROS 602 has important advantages. For example, it accommodates limited resource execution environments such as provided by a lower cost SPU 500. It also provides an extremely high level of configurability. In fact, ROS 602 will accommodate an almost unlimited diversity of content types, content provider objectives, transaction types and client requirements. In addition, the ability to dynamically assemble independently deliverable components at execution time based on particular objects and users provides a high degree of flexibility" ('193 87:63 - 88:7) 9. "Each logical object structure 800 may also include a 'private body' 806 containing or referencing a set of methods 1000 (i.e., programs or procedures) that control use and distribution of the object 300. The ability to optionally incorporate different methods 1000 with each object is important to making VDE 100 highly configurable." ('193 128:25-30) 10. "VDE methods 1000 are designed to provide a very flexible and highly modular approach to secure processing." ('193 181:17-18) 11. "The reusable functional primitives of VDE 100 can be flexibly combined by content providers to reflect their respective distribution objectives." ('193 255:27-29) 12. "The present invention truly achieves a content control and auditing architecture that can be configured to most any commercial distribution embodiment." ('193 261:12-15) 13. "Adding new content to objects is an important aspect of authoring provided by the present invention. Providers may wish to allow one or more users to add, hide, modify, remove and/or extend content that they provide. In this way, other users may add value to, alter for a new purpose, maintain, and/or otherwise change, existing content. The ability to add content to an empty and/or newly created object is important as well." ('193 261:23-30) 14. "The distribution control information provided by the present invention allows flexible positive control. No provider is required to include any particular control, or use any particular strategy, except as required by senior control information. Rather, the present invention allows a provider to select from generic control components (which may be provided as a subset of components appropriate to a provider's specific market, for example, as included in and/or directly compatible with, a VDE application) to establish a structure appropriate for a given chain of handling/control." ('193 263:9-19)" 15. "Importantly, VDE securely and flexibly supports editing the content in, extracting content from, embedding content into, and otherwise shaping the content composition of, VDE content containers. Such capabilities allow VDE supported product models to evolve by progressively reflecting the

	Claim Term/Phrase	Evidence Supporting MS Construction
		requirements of 'next' participants in an electronic commercial model." ('193 297:9-15) 16. "For instance, the user may have an 'access'right, and an 'extraction' right, but not a 'copy' right." ('193 159:24-26) 17. "PERCS 808 specify a set of rights that may be exercised to use or access the corresponding VDE object 300. The preferred embodiment allows users to 'customize' their access rights by selecting a subset of rights authorized by a corresponding PERC 808 and/or by specifying parameters or choices that correspond to some or all of the rights granted by PERC 808. These user choices are set forth in a user rights table 464 in the preferred embodiment. User rights table (URT) 464 includes URT records, each of which correspond to a user (or group of users). Each of these URT records specific users choices for a corresponding VDE object more methods 1000 for exercising the rights granted to the user by the PERC 808 in a way specified by the choices contained within the URT record." ('193 156:55 - 157:3) 18. "PERC and URT structures provide a mechanism that may be used to provide precise electronic representation of rights and the controls associated with those rights. VDE thus provides a 'vocabulary' and mechanism by which users and creators may specify their desires." ('193 245:10-15) 19. "In sum, the present invention allows information contained in electronic information products to be supplied according to user specification. Tailoring to user specification allows the present invention to provide the greatest value to users, which in turn will generate the greatest amount of electronic commerce activity." ('193 22:66 - 23:5) 20. "Adding new content to objects is an important aspect of authoring provided by the present invention. Providers may wish to allow one or more users to add, hide, modify, remove and/or extend content that they provide. In this way, other users may add value to, alter for a new purpose, maintain, and/otherwise change, existing content. The ability to add content to an empty and/or newly created object is important as well." ('193 261:23-30) 21. "Each logical object structure 800 may also include a 'private body' 806 containing or referencing a set of method 1000 (i.e., programs or procedures) that control use and distribution of the object 300. The ability to optionally incorporate different methods 1000 with each object is important to making VDE 100 highly configurable." ('193 128:25-30) 22. "An important aspect of adding or modifying content is the choice of encryption/decryption keys and/or other relevant aspects of securing new or altered content." ('193 262:21-23) (9) GENERAL PURPOSE; UNIVERSAL: **Intrinsic:** 1. "VDE also features fundamentally important capabilities for managing content that travels 'across' the 'information highway.' These capabilities comprise a rights protection solution that serves all electronic community members. These members include content creators and distributors, financial service providers, end-users, and others. VDE is the first general purpose,

	Claim Term/Phrase	Evidence Supporting MS Construction
		configurable, transaction control/rights protection solution for users of computers, other electronic appliances, networks, and the information highway." ('193 2:27-36) 2. "VDE provides a unified solution that allows all content creators, providers, and users to employ the same electronic rights protection solution." ('193 5:17-19) 3. "Since different groups of components can be put together for different applications, the present invention can provide electronic control information for a wide variety of different products and markets. This means the present invention can provide a 'unified,' efficient, secure, and cost-effective system for electronic commerce and data security. This allows VDE to serve as a single standard for electronic rights protection, data security, and electronic currency and banking." ('193 7:6-14) 4. "Employing VDE as a general purpose electronic transaction/distribution control system allows users to maintain a single transaction management control arrangement on each of their computers, networks, communication nodes, and/or other electronic appliances. Such a general purpose system can serve the needs of many electronic transaction management applications without requiring distinct, different installations for different purposes. As a result, users of VDE can avoid the confusion and expense and other inefficiencies of different, limited purpose transaction control applications for each different content and/or business model. For example, VDE allows content creators to use the same VDE foundation control arrangement for both content authoring and for licensing content from other content creators for inclusion into their products or for other use. Clearinghouses, distributors, content creators, and other VDE users can all interact, both with the applications running on their VDE installations, and with each other, in an entirely consistent manner, using and reusing (largely transparently) the same distributed tools, mechanisms, and consistent user interfaces, regardless of the type of VDE activity." ('193 11:38-59) 5. "An objective of VDE is supporting a transaction/distribution control standard." ('193 15:66-67) 6. "Summary of Some Important Features Provided by VDE in Accordance With the Present Invention ... The design of the VDE foundation, VDE load modules, and VDE containers, are important features that enable the VDE node operating environment to be compatible with a very broad range of electronic appliances. The ability, for example, for control methods based on load modules to execute in very 'small' and inexpensive secure sub-system environments, such as environments with very little read/write memory, while also being able to execute in large memory sub-systems that may be used in more expensive electronic appliances, supports consistency across many machines. This consistent VDE operating environment, including its control structures and container architecture, enables the use of standardized VDE content containers across a broad range of device types and host operating environments. Since VDE capabilities can be seamlessly integrated as extensions, additions, and/or modifications to fundamental capabilities of

	Claim Term/Phrase	Evidence Supporting MS Construction
		electronic appliances and host operating systems, VDE containers, content control information, and the VDE foundation will be able to work with many device types and these device types will be able to consistently and efficiently interpret and enforce VDE control information." ('193 21:43-46; 34:26-49) 7. "This rationalization stems from the reusability of control structures and user interfaces for a wide variety of transaction management related activities. As a result, content usage control, data security, information auditing, and electronic financial activities, can be supported with tools that are reusable, convenient, consistent, and familiar. In addition, a rational approach--a transaction/distribution control standard--allows all participants in VDE the same foundation set of hardware control and security, authoring, administration, and management tools to support widely varying types of information, business market model, and/or personal objectives." ('193 11:26-37) 8. "Because of the breadth of issues resolved by the present invention, it can provide the emerging 'electronic highway' with a single transaction/ distribution control system that can, for a very broad range of commercial and data security models, ensure against unauthorized use of confidential and/or proprietary information and commercial electronic transactions. VDE's electronic transaction management mechanisms can enforce the electronic rights and agreements of all parties participating in widely varying business and data security models, and this can be efficiently achieved through a single VDE implementation within each VDE participant's electronic appliance. VDE supports widely varying business and/or data security models that can involve a broad range of participants at various 'levels' of VDE content and/or content control information pathways of handling. Different content control and/or auditing models and agreements may be available on the same VDE installation. These models and agreements may control content in relationship to, for example, VDE installations and/or users in general; certain specific users, installations, classes and/or other groupings of installations and/or users; as well as to electronic content generally on a given installation, to specific properties, property portions, classes and/or other groupings of content." ('193 17:22-45) 9. "The present invention's trusted/secure, universe wide, distributed transaction control and administration system." ('193 35:66 - 36:1) 10. "Commerce Utility Systems 90 are generalized and programmable..." ('712 67:7-8) (10) <u>FLEXIBLE</u>: **Intrinsic:** 1. "Providers of 'electronic currency' have also created protections for their type of content. These systems are not sufficiently adaptable, efficient, nor flexible enough to support the generalized use of electronic currency. Furthermore, they do not provide sophisticated auditing and control configuration capabilities. This means that current electronic currency tools lack the sophistication needed

	Claim Term/Phrase	Evidence Supporting MS Construction
		for many real-world financial business models. VDE provides means for anonymous currency and for 'conditionally' anonymous currency, wherein currency related activities remain anonymous except under special circumstances." ('193 3:10-20) 2. "Traditional content control mechanisms often require users to purchase more electronic information than the user needs or desires. For example, infrequent users of shrink-wrapped software are required to purchase a program at the same price as frequent users, even though they may receive much less value from their less frequent use. Traditional systems do not scale cost according to the extent or character of usage and traditional systems can not attract potential customers who find that a fixed price is too high. Systems using traditional mechanisms are also not normally particularly secure. For example, shrink-wrapping does not prevent the constant illegal pirating of software once removed from either its physical or electronic package." ('193 5:50-62) 3. "Traditional electronic information rights protection systems are often inflexible and inefficient and may cause a content provider to choose costly distribution channels that increase a product's price. In general these mechanisms restrict product pricing, configuration, and marketing flexibility. These compromises are the result of techniques for controlling information which cannot accommodate both different content models and content models which reflect the many, varied requirements, such as content delivery strategies, of the model participants. This can limit a provider's ability to deliver sufficient overall value to justify a given product's cost in the eyes of many potential users. VDE allows content providers and distributors to create applications and distribution networks that reflect content providers' and users' preferred business models. It offers users a uniquely cost effective and feature rich system that supports the ways providers want to distribute information and the ways users want to use such information." ('193 5:63 - 6:13) 4. "VDE does not require electronic content providers and users to modify their business practices and personal preferences to conform to a metering and control application program that supports limited, largely fixed functionality. Furthermore, VDE permits participants to develop business models not feasible with non- electronic commerce, for example, involving detailed reporting of content usage information, large numbers of distinct transactions at hitherto infeasible low price points, 'pass-along' control information that is enforced without involvement or advance knowledge of the participants, etc." ('193 9:67 - 10:9) 5. "VDE can further be used to enable commercially provided electronic content to be made available to users in user defined portions, rather than constraining the user to use portions of content that were 'predetermined' by a content creator and/or other provider for billing purposes." ('193 11:66 - 12:4) 6. "The 'usage map' concept provided by the preferred embodiment may be tied to the concept of 'atomic elements.' In the preferred embodiment, usage of an object 300 may be metered in terms of 'atomic elements.' In the preferred embodiment, an 'atomic element' in the metering context defines a unit of usage that is 'sufficiently significant' to be recorded in a meter. The definition

	Claim Term/Phrase	Evidence Supporting MS Construction
		of what constitutes an 'atomic element' is determined by the creator of an object 300. For instance, a 'byte' of information content contained in an object 300 could be defined as an 'atomic element,' or a record of a database could be defined as an 'atomic element,' or each chapter of an electronically published book could be defined as an 'atomic element.'" ('193 144:53-65) 7. "Summary of Some Important Features Provided by VDE in Accordance With the Present Invention. VDE employs a variety of capabilities that serve as a foundation for a general purpose, sufficiently secure distributed electronic commerce solution. VDE enables an electronic commerce marketplace that supports divergent, competitive business partnerships, agreements, and evolving overall business models. For example, VDE includes features that. . . support dynamic user selection of information subsets of a VDE electronic information product (VDE controlled content). This contrasts with the constraints of having to use a few high level individual, pre-defined content provider information increments such as being required to select a whole information product or product section in order to acquire or otherwise use a portion of such product or section. VDE supports metering and usage control over a variety of increments (including 'atomic' increments, and combinations of different increment types) that are selected ad hoc by a user and represent a collection of pre-identified one or more increments (such as one or more blocks of a preidentified nature, e.g., bytes, images, logically related blocks) that form a generally arbitrary, but logical to a user, content 'deliverable.' VDE control information (including budgeting, pricing and metering) can be configured so that it can specifically apply, as appropriate, to ad hoc selection of different, unanticipated variable user selected aggregations of information increments and pricing levels can be, at least in part, based on quantities and/or nature of mixed increment selections (for example, a certain quantity of certain text could mean associated images might be discounted by 15%; a greater quantity of text in the 'mixed' increment selection might mean the images are discounted 20%). Such user selected aggregated information increments can reflect the actual requirements of a user for information and is more flexible than being limited to a single, or a few, high level, (e.g. product, document, database record) predetermined increments. Such high level increments may include quantities of information not desired by the user and as a result be more costly than the subset of information needed by the user if such a subset was available. In sum, the present invention allows information contained in electronic information products to be supplied according to user specification. Tailoring to user specification allows the present invention to provide the greatest value to users, which in turn will generate the greatest amount of electronic commerce activity. The user, for example, would be able to define an aggregation of content derived from various portions of an available content product, but which, as a deliverable for use by the user, is an entirely unique aggregated increment. The user may, for example, select certain numbers of bytes of information from various portions of an information product, such as a reference work, and copy them to disc in unencrypted form and be billed based on total number of bytes plus a surcharge on the number of 'articles' that provided the bytes. A content provider might

	Claim Term/Phrase	Evidence Supporting MS Construction
		reasonably charge less for such a user defined information increment since the user does not require all of the content from all of the articles that contained desired information." ('193 21:43-53; 22:32-49) 8. "Summary of Some Important Features Provided by VDE in Accordance With the Present Invention ... Differing models for billing, auditing, and security can be applied to the same piece of electronic information content and such differing sets of control information may employ, for control purposes, the same, or differing, granularities of electronic information control increments." ('193 21:43-46; 28:23-28) 9. "The VDE templates, classes, and control structures are inherently flexible and configurable to reflect the breadth of information distribution and secure storage requirements, to allow for efficient adaptation into new industries as they evolve, and to reflect the evolution and/or change of an existing industry and/or business, as well as to support one or more groups of users who may be associated with certain permissions and/or budgets and object types. The flexibility of VDE templates, classes, and basic control structures is enhanced through the use of VDE aggregate and control methods which have a compound, conditional process impact on object control. Taken together, and employed at times with VDE administrative objects and VDE security arrangements and processes, the present invention truly achieves a content control and auditing architecture that can be configured to most any commercial distribution embodiment. Thus, the present invention fully supports the requirements and biases of content providers without forcing them to fit a predefined application model. It allows them to define the rights, control information, and flow of their content (and the return of audit information) through distribution channels." ('193 260:66 - 261:20) 10. "VDE also extends usage control information to an arbitrary granular level (as opposed to a file based level provided by traditional operating systems) and provides flexible control information over any action associated with the information which can be described as a VDE controlled process." ('193 275:8-13) 11. "The situation is no better for processing documents within the context of ordinary computer and network systems. Although said systems can enforce access control information based on user identity, and can provide auditing mechanisms for tracking accesses to files, these are low-level mechanisms that do not permit tracking or controlling the flow of content. In such systems, because document content can be freely copied and manipulated, it is not possible to determine where document content has gone, or where it came from. In addition, because the control mechanisms in ordinary computer operating systems operate at a low level of abstraction, the entities they control are not necessarily the same as those that are manipulated by users. This particularly causes audit trails to be cluttered with voluminous information describing uninteresting activities." ('193 281:27-41) 12. "Importantly, VDE securely and flexibly supports editing the content in, extracting content from, embedding content into, and otherwise shaping the content composition of, VDE content containers." ('193 297:9-12)

	Claim Term/Phrase	Evidence Supporting MS Construction
		13. "The InterTrust DigiBox container model allows and facilitates these and other different container uses. It facilitates detailed container customization for different uses, classes of use and/or users in order to meet different needs and business models. This customization ability is very important, particularly when used in conjunction with a general purpose, distributed rights management environment such as described in Ginter, et al. Such an environment calls for a practical optimization of customizability, including customizability and transparency for container models. This customization flexibility has a number of advantages, such as allowing optimization (e.g., maximum efficiency, minimum overhead) of the detailed container design for each particular application or circumstance so as to allow many different container designs for many different purposes (e.g., business models) to exist at the same time and be used by the rights control client (node) on a user electronic appliance such as a computer or entertainment device." ('861 2:49-67) 14. "The node and container model described above and in the Ginter et al. patent specification (along with similar other DigiBox/VDE (Virtual Distribution Environment) models) has nearly limitless flexibility." ('861 2:37-40) 15. "Such capabilities allow VDE supported product models to evolve by progressively reflecting requirements of 'next' participants in an electronic commercial models." ('193 297:12-15)
25.	193.1: "a budget specifying the number of copies which can be made of said digital file"	**Intrinsic:** 1. "For example, content control information for a given piece of content may be stipulated as senior information and therefore not changeable, might be put in place by a content creator and might stipulate that national distributors of a given piece of their content may be permitted to make 100,000 copies per calendar quarter, so long as such copies are provided to bonfire end-users, but may pass only a single copy of such content to a local retailers and the control information limits such a retailer to making no more than 1,000 copies per month for retail sales to end-users. In addition, for example, an end-user of such content might be limited by the same content control information to making three copies of such content, one for each of three different computers he or she uses (one desktop computer at work, one for a desktop computer at home, and one for a portable computer)." ('193 48:19-34) 2. "... storing a first digital file and a first control in a first secure container, said first control constituting a first budget which governs the number of copies which may be made of said first digital file or a portion of said first digital file while said first digital file is contained in said first secure container," ('193 claim 60) 3. "A certain content provider might, for example, require metering the number of copies made for distribution to employees of a given software program (a portion of the program might be maintained in encrypted form and require the presence of a VDE installation to run). This would require the execution of a metering method for copying of the property each time a copy was made for another employee." ('193 20:36-43) 4. "For example, in the earlier example of a user with a desktop and a notebook computer, a provider may allow a user to make copies of information necessary to enable the notebook computer based on information present in the desktop

	Claim Term/Phrase	Evidence Supporting MS Construction
		computer, but not allow any further copies of said information to be made by the notebook VDE node. In this example, the distribution control structure described earlier would continue to exist on the desktop computer, but the copies of the enabling information passed to the notebook computer would lack the required distribution control structure to perform distribution from the notebook computer. Similarly, a distribution control structure may be provided by a content provider to a content provider who is a distributor in which a control structure would enable a certain number of copies to be made of a VDE content container object along with associated copies of permissions records, but the permissions records would be altered (as per specification of the content provider, for example) so as not to allow end-users who received distributor created copies from making further copies for distribution to other VDE nodes." ('193 264:29-49) 5. "SPU 500 is enclosed within and protected by a 'tamper resistant security barrier' 502. Security barrier 502 separates the secure environment 503 from the rest of the world. It prevents information and processes within the secure environment 503 from being observed, interfered with and leaving except under appropriate secure conditions." ('193 59:48-53) 6. "Secure container 302 may also contain an electronic, digital control structure 4078. This control structure 4078 (which could also be delivered independently in another container 302 different from the one carrying the image 4068I and/or the data 4068D) may contain important information controlling use of container 302. For example, controls 4078 may specify who can open container 302 and under what conditions the container can be opened. Controls 4078 might also specify who, if anyone, object 300 can be passed on to. As another example, controls 4078 might specify restrictions on how the image 4068I and/or data 4068D can be used (e.g., to allow the recipient to view but not change the image and/or data as one example). The detailed nature of control structure 4078 is described in connection, for example, with FIGS. 11D-11J ; FIG. 15 ; FIGS. 17-26B; and FIGS. 41A-61." ('683 25:62–26:10) 7. "Many objects 300 that are distributed by physical media and/or by 'out of channel' means (e.g., redistributed after receipt by a customer to another customer) might not include key blocks 810 in the same object 300 that is used to transport the content protected by the key blocks. This is because VDE objects may contain data that can be electronically copied outside the confines of a VDE node. If the content is encrypted, the copies will also be encrypted and the copier cannot gain access to the content unless she has the appropriate decryption key(s)." ('193 128:66) 8. "Although block 1262 includes encrypted summary services information on the back up, it preferably does not include SPU device private keys, shared keys, SPU code and other internal security information to prevent this information from ever becoming available to users even in encrypted form." ('193 166:59-64)
26.	193.1: "controlling the copies made of said digital file"	See above.

	Claim Term/Phrase	Evidence Supporting MS Construction
27.	721.1: "digitally signing a second load module with a second digital signature different from the first digital signature, the second digital signature designating the second load module for use by a second device class having at least one of tamper resistance and security level different from the at least one of tamper resistance and security level of the first device class"	**Intrinsic:** 1. "In one example, verifying authority 100 may digitally sign identical copies of load module 54 for use by different classes or 'assurance levels' of electronic appliances 61." ('721 18:19-22) 2. "Protected execution spaces such as protected processing environments can be programmed or otherwise conditioned to accept only those load modules or other executables bearing a digital signature/certificate of an accredited (or particular) verifying authority. Tamper resistant barriers may be used to protect this programming or other conditioning. The assurance levels described below are a measure or assessment of the effectiveness with which this programming or other conditioning is protected." ('721 5:1-9) 3. "For example, protected processing environments or other secure execution spaces that are more impervious to tampering (such as those providing a higher degree of physical security) may use an assurance level that isolates it from protected processing environments or other secure execution spaces that are relatively more susceptible to tampering (such as those constructed solely by software executing on a general purpose digital computer in a non-secure location)." ('721 6:34-41) 4. "The present invention may use a verifying authority and the digital signatures it provides to compartmentalize the different electronic appliances depending on their level of security (e.g., work factor or relative tamper resistance)." ('721 6:53-56) 5. "Assurance level I might be used for an electronic appliance(s) 61 whose protected processing environment 108 is based on software techniques that may be somewhat resistant to tampering. An example of an assurance level I electronic appliance 61A might be a general purpose personal computer that executes software to create protected processing environment 108. An assurance level II electronic appliance 61B may provide a protected processing environment 108 based on a hybrid of software security techniques and hardware-based security techniques. An example of an assurance level II electronic appliance 61B might be a general purpose personal computer equipped with a hardware integrated circuit secure processing unit ('SPU') that performs some secure processing outside of the SPU (see Ginter et al. patent disclosure FIG. 10 and associated text). Such a hybrid arrangement might be relatively more resistant to tampering than a software-only implementation. The assurance level III appliance 61C shown is a general purpose personal computer equipped with a hardware-based secure processing unit 132 providing and completely containing protected processing environment 108 (see Ginter et al. FIGS. 6 and 9 for example). A silicon-based special purpose integrated circuit security chip is relatively more tamper-resistant than implementations relying on software techniques for some or all of their tamper-resistance." ('721 6:44 – 7:5) 6. "Assurance level in this example may be assigned to a particular protected processing environment 108 at initialization (e.g., at the factory in the case of hardware-based secure processing units). Assigning assurance level at initialization time facilitates the use of key management (e.g., secure key exchange protocols) to enforce isolation based on assurance level. For example,

	Claim Term/Phrase	Evidence Supporting MS Construction
		since establishment of assurance level is done at initialization time, rather than in the field in this example, the key exchange mechanism can be used to provide new keys (assuming an assurance level has been established correctly)." ('721 17:13-23)
28.	891.1: "securely applying, at said first appliance through use of said at least one resource said first entity's control and said second entity's control to govern use of said data item"	**Intrinsic:** 1. "Such secure combination of VDE manage pieces of content will frequently require VDE's ability to securely derive content control information which accommodates the control information requirements, including any combinational rules, of the respective VDE managed pieces of content and reflects an acceptable agreement between plural control information sets." ('193 296:26-32)
29.	900.155: "derives information from one or more aspects of said host processing environment"	**Intrinsic:** 1. See '900 73:1- 80:6 a. "SPU Integrated Within CPU b. As discussed above, it may be desirable to integrate CPU 654 and SPU 500 into the same integrated circuit and/or device. SPU 500 shown in FIG. 9 includes a microprocessor 520 that may be similar or identical to a standard microprocessor available off-the-shelf from a variety of manufacturers. Similarly, the SPU DMA controller 526 and certain other microprocessor support circuitry may be standard implementations available in off-the-shelf microprocessor and/or microcomputer chips. Since many of the general control and processing requirements provided by SPU 500 in the preferred embodiment can be satisfied using certain generic CPU and/or microcontroller components, it may be desirable to integrate SPU VDE functionality into a standard generic CPU or microcontroller chip. Such an integrated solution can result in a very cost-effective 'dual mode' component that is capable of performing all of the generic processing of a standard CPU as well as the secure processing of an SPU. Many of the control logic functions performed by the preferred embodiment SPU can be performed by generic CPU and/or micro-controller logic so that at least a portion of the control logic does not have to be duplicated. Additional cost savings (e.g., in terms of reducing manufacturing costs, inventory costs and printed circuit board real estate requirements) may also be obtained by not requiring an additional, separate physical SPU 500 device or package. FIG. 9A shows one example architecture of a combination CPU/SPU 2650. CPU/SPU

	Claim Term/Phrase	Evidence Supporting MS Construction
		2650 may include a standard microprocessor or microcontroller 2652, a standard bus interface unit (BIU) 2656, and a standard (optional) DMA controller 2654, as well as various other standard I/O controllers, computation circuitry, etc. as may be found in a typical off-the-shelf microprocessor/microcontroller. Real time clock 528 may be added to the standard architecture to give the CPU/SPU 2650 access to the real time clock functions as discussed above in connection with FIG. 9. Real-time clock 528 must be protected from tampering in order to be secure. Such protections may include internal or external backup power, an indication that its power (and thus its operation) has been interrupted, and/or an indication that the external clock signal(s) from which it derives its timing have been interfered with (e.g., sped up, slowed down). Similarly, an encrypt/decrypt engine 522, pattern matching engine 524, compression/decompression engine 546 and/or arithmetic accelerator 544 may be added if desired to provide greater efficiencies, or the functions performed by these components could be provided instead by software executing on microprocessor 2652. An optional memory management unit 540 may also be provided if desired. A true random number generator 542 may be provided also if desired. Connections shown between mode interface switch 2658 and other components can carry both data and control information, specifically control information that determines what security-relevant aspects of the other components are available for access and/or manipulation. c. In addition, secure ROM 532 and/or secure RAM 534 may be provided within CPU/SPU 2650 along with a 'mode interface switch' 2658a, 2658b. Mode interface switch 2658 selectively provides microprocessor 2652 with access to secure memory 532, 534 and other secure components (blocks 522, 546, 524, 542, 544, 528) depending upon the 'mode' CPU/SPU 2650 is operating in. CPU/SPU 2650 in this example may operate in two different modes: an 'SPU' mode, or a 'normal' mode. In the 'normal' mode, CPU/SPU 2650 operates substantially identically to a standard off-the-shelf CPU while also protecting the security of the content, state, and operations of security-relevant components included in CPU/SPU 2650. Such security-relevant components may include the secure memories 532, 534; the encrypt/decrypt engine 522, the optional pattern-matching engine 524, random number generator 542, arithmetic accelerator 544, the SPU-not-initialized flag 2671, the secure mode interface switch 2658, the real-time clock 528, the DMA controller 2654, the MMU 540, compress/decompress block 546, and/or any other components that may affect security of the operation of the CPU/SPU in 'SPU' mode. d. In this example, CPU/SPU 2650 operating in the 'normal' mode controls mode interface switch 2658 to effectively 'disconnect' (i.e., block unsecure access to) the security-relevant components, or to the security-relevant aspects of the operations of such components as have a function for both 'normal' and 'SPU' mode. In the 'normal' mode, for

	Claim Term/Phrase	Evidence Supporting MS Construction
		example, microprocessor 2652 could access information from standard registers or other internal RAM and/or ROM (not shown), execute instructions in a 'normal' way, and perform any other tasks as are provided within a standard CPU--but could not access or compromise the contents of secure memory 532, 534 or access blocks 522, 524, 542, 544, 546. In this example 'normal' mode, mode interface switch 2658 would effectively prevent any access (e.g., both read and write access) to secure memory 532, 534 so as to prevent the information stored within that secure memory from being compromised. e. When CPU/SPU 2650 operates in the 'SPU' mode, mode interface switch 2658 allows microprocessor 2652 to access secure memory 532, 534, and to control security-relevant aspects of other components in the CPU/SPU. The 'SPU' mode in this example requires all instructions executed by microprocessor 2652 to be fetched from secure memory 532, 534--preventing execution based on 'mixed' secure and non-secure instructions. In the 'SPU' mode, mode interface switch 2658 may, in one example embodiment, disconnect or otherwise block external accesses carried over bus 652 from outside CPU/SPU 2650 (e.g., DMA accesses, cache coherency control accesses) to ensure that the microprocessor 2652 is controlled entirely by instructions carried within or derived from the secure memory 532, 534. Mode interface switch 2658 may also disconnect or otherwise block access by microprocessor 2652 to some external memory and/or other functions carried over bus 652. Mode interface switch 2658 in this example prevents other CPU operations/instructions from exposing the contents of secure memory 532, 534. f. In the example shown in FIG. 9A, the mode control of mode interface switch 2658 is based on a 'mode' control signal provided by microprocessor 2652. In this example, microprocessor 2652 may be slightly modified so it can execute two 'new' instructions: 'enable `SPU` mode' instruction, and 'disable `SPU` mode' instruction. g. When microprocessor 2652 executes the 'enable `SPU` mode' instruction, it sends an appropriate 'mode' control signal to mode interface switch 2658 to 'switch' the interface switch into the 'SPU' mode of operation. When microprocessor 2652 executes the 'disable `SPU` mode' instruction, it sends an appropriate 'mode' control signal to mode interface switch 2658 to disable the 'SPU' mode of operation. h. When CPU/SPU 2650 begins operating in the 'SPU' mode (based on microprocessor 2652 executing the 'enable 'SPU' mode' instruction), mode interface switch 2658 forces microprocessor 2652 to begin fetching instructions from secure memory 532, 534 (e.g., beginning at some fixed address) in one example. When CPU/SPU 2650 begins operating in this example 'SPU' mode, mode interface switch 2658 may force microprocessor 2652 to load its registers from some fixed address in secure memory 532, 534 and may begin execution based on such register content. Once operating in the 'SPU' mode, microprocessor 2652 may

	Claim Term/Phrase	Evidence Supporting MS Construction
		provide encryption/decryption and other control capabilities based upon the code and other content of secure memory 532, 534 needed to provide the VDE functionality of SPU 500 described above. For example, microprocessor 2652 operating under control of information within secure memory 532, 534 may read encrypted information from bus 652 via bus interface unit 2656, write decrypted information to the bus interface unit, and meter and limit decryption of such information based on values stored in the secure memory. i. At the end of secure processing, execution by microprocessor 2652 of the 'disable SPU mode' instruction may cause the contents of all registers and other temporary storage locations used by microprocessor 2652 that are not within secure memory 532, 534 to be destroyed or copied into secure memory 532, 534 before 'opening' mode interface switch 2658. Once mode interface switch 2658 is 'open,' the microprocessor 2652 no longer has access to secure memory 532, 534 or the information it contained, or to control or modify the state of any other security-relevant components or functions contained within CPU/SPU 2650 to which access is controlled by mode interface switch 2658. j. Whenever CPU/SPU 2650 enters or leaves the 'SPU' mode, the transition is performed in such a way that no information contained in the secure memory 532, 534 or derived from it (e.g., stored in registers or a cache memory associated with microprocessor 2652) while in the 'SPU' mode can be exposed by microprocessor 2652 operations that occur in the 'normal' mode. This may be accomplished either by hardware mechanisms that protect against such exposure, software instructions executed in 'SPU' mode that clear, reinitialize, and otherwise reset during such transitions, or a combination of both. k. In some example implementations, interrupts may be enabled while CPU/SPU 2650 is operating in the 'SPU' mode similarly interrupts and returns from interrupts while in the 'SPU' mode may allow transitions from 'SPU' mode to 'normal' mode and back to 'SPU' mode without exposing the content of secure memory 532, 534 or the content of registers or other memory associated with microprocessor 2652 that may contain information derived from secure mode operation. l. In some example implementations, there may be CPU/SPU activities such as DMA transfers between external memory and/or devices and secure memory 532, 534 that are initiated by microprocessor 2652 but involve autonomous activity by DMA controller 2654 and, optionally, encrypt/decrypt engine 522 and/or compress/decompress engine 546. In such implementations, mode interface switch 2658 and its associated control signals may be configured to permit such pending activities (e.g. DMA transfers) to continue to completion even after CPU/SPU 2650 leaves 'SPU' mode, provided that upon completion, all required clearing, reinitialization, and/or reset activities occur, and provided that no access or interference is permitted with the pending activities except when CPU/SPU 2650 is operating in 'SPU' mode.

	Claim Term/Phrase	Evidence Supporting MS Construction
		m. In an additional example embodiment, encryption/decryption logic may be connected between microprocessor 2652 and secure memory 532, 354. This additional encryption/decryption logic may be connected 'in parallel' to mode interface switch 2658. The additional encryption/decryption logic may allow certain accesses by microprocessor 2652 to the secure memory 532, 534 when CPU/SPU 2650 is operating in the 'normal' mode. In this alternate embodiment, reads from secure memory 532, 534 when CPU/SPU 2650 is operating in the 'normal' mode automatically result in the read information being encrypted before it is delivered to microprocessor 2652 (and similarly, and writes to the secure memory may result in the written information being decrypted before it is deposited into the secure memory). This alternative embodiment may permit access to secure memory 532, 534 (which may in this example store the information in 'clear' form) by microprocessor 2652 when CPU/SPU 2650 is operating in the 'non-secure normal' mode, but only reveals the secure memory contents to microprocessor 2652 in unencrypted form when the CPU/SPU is operating in the 'SPU' mode. Such access may also be protected by cryptographic authentication techniques (e.g., message authentication codes) to prevent modification or replay attacks that modify encrypted data stored in secure memory 532, 534. Such protection may be performed utilizing either or both of software and/or hardware cryptographic techniques. n. All of the components shown in FIG. 9A may be disposed within a single integrated circuit package. Alternatively, mode interface switch 2658 and secure memory 532, 534, and other security-relevant components might be placed within an integrated circuit chip package and/or other package separate from the rest of CPU/SPU 2650. In this two-package version, a private bus could be used to connect microprocessor 2652 to the mode interface switch 2658 and associated secure memory 532, 534. To maintain security in such multi-package versions, it may be necessary to enclose all the packages and their interconnections in an external physical tamper-resistant barrier. o. Initialization of Integrated CPU/SPU p. Instructions and/or data may need to be loaded into CPU/SPU 2650 before it can operate effectively as an SPU 500. This may occur during the manufacture of CPU/SPU 2650 or subsequently at a CPU/SPU initialization facility. Security of such initialization may depend on physical control of access to the CPU/SPU component(s), on cryptographic means, or on some combination of both. Secure initialization may be performed in plural steps under the control of different parties, such that an initialization step to be performed by party B is preconditioned on successful performance of a step by party A. Different initialization steps may be protected using different security techniques (e.g. physical access, cryptography). q. In this example, switch 2658 may expose an external control signal 2670 that requests operation in 'SPU' mode rather than 'normal'

	Claim Term/Phrase	Evidence Supporting MS Construction
		mode after a power-on reset. This signal would be combined (e.g., by a logical AND 2672) with a non-volatile storage element 2671 internal to CPU/SPU 2650. If both of these signals are asserted, AND gate 2672 would cause CPU/SPU 2650 to begin operating in SPU mode, either executing existing instructions from an address in SPU memory 532, executing instructions from main memory 2665 or otherwise external to the CPU/SPU. The instructions thus executed would permit arbitrary initialization and other functions to be performed in 'SPU' mode without necessarily requiring any instructions to be previously resident in the SPU memory 532. r. Once initialized, the SPU would, under control of its initialization program, indicate to switch 2658 that the flag 2671 is to be cleared. Clearing flag 2671 would permanently disable this initialization capability because no mechanism would be provided to set flag 2671 back to its initial value. If flag 2671 is clear, or control signal 2670 is not asserted, CPU/SPU 2650 would behave precisely as does microprocessor 2652 with respect to power-on reset and other external conditions. Under such conditions, only execution of the 'enable SPU mode' instruction or otherwise requesting SPU mode under program control would cause 'SPU' mode to be entered. s. Additionally, a mechanism could be provided to permit microprocessor 2652 and/or control signal 2672 to reinitialize the flag 2671. Such reinitialization would be performed in a manner that cleared secure memory 532, 534 of any security-relevant information and reinitialized the state of all security-relevant components. This reinitialization mechanism would permit CPU/SPU 2650 to be initialized several times, facilitating testing and/or re-use for different applications, while protecting all security-relevant aspects of its operation. t. In the preferred embodiment, CPU/SPU 2650 would, when SPU mode has not yet been established, begin operating in SPU mode by fetching instructions from secure non-volatile memory 532, thereby ensuring a consistent initialization sequence and preventing SPU dependence on any information held outside CPU/SPU 2650. This approach permits secret initialization information (e.g., keys for validating digital signatures on additional information to be loaded into secure memory 532, 534) to be held internally to CPU/SPU 2650 so that it is never exposed to outside access. Such information could even be supplied by a hardware 'mask' used in the semiconductor fabrication process. u. CPU/SPU Integrated With Unmodified Microprocessor v. FIG. 9B shows an additional example embodiment, in which a completely standard microprocessor 2652 integrated circuit chip could be transformed into a CPU/SPU 2650 by adding an SPU chip 2660 that mediates access to external I/O devices and memory. In such an embodiment, the microprocessor 2652 would be connected to the SPU chip 2660 by a private memory bus 2661, and all three such components would be contained within hardware tamper-resistant barrier 502.

	Claim Term/Phrase	Evidence Supporting MS Construction
		w. In this embodiment, SPU chip 2660 may have the same secure components as in FIG. 9, i.e., it may have a ROM/EEPROM 532, a RAM 532, an RTC 528, an (optional) encryption/decryption engine 522, an (optional) random number generator (RNG) 542, an (optional) arithmetic accelerator 544, and a (optional) compression/decompression engine 546, and a (optional) pattern matching circuit 524. Microprocessor 520 is omitted from SPU chip 2660 since the standard microprocessor 2650 performs the processing functions instead. In addition, SPU chip 2660 may include a flag 2671 and AND gate logic 2672 for the initialization purposes discussed above. x. In addition, SPU chip 2660 includes an enhanced switch 2663 that provides the same overall (bus enhanced) functionality performed by the switch 2658 in the FIG. 9A embodiment. y. Enhanced switch 2663 would perform the functions of a bus repeater, mediator and interpreter. For example, enhanced switch 2663 may act as a bus repeater that enables microprocessor 2652's memory accesses made over internal memory bus 2661 to be reflected to external memory bus 2664 and performed on main memory 2665. Enhanced switch 2663 may also act as a bus repeater similarly for internal I/O bus 2662 to external I/O bus 2665 in the event that microprocessor 2652 performs I/O operations distinctly from memory operations. Enhanced switch 2663 may also perform the function of a mediator for microprocessor control functions 2666 (e.g., non-maskable interrupt, reset) with respect to externally requested control functions 2667. Enhanced switch 2663 may also provide mediation for access to SPU-protected resources such as ROM 532, RAM 534, encrypt/decrypt engine 522 (if present), random number generator 542 (if present), arithmetic accelerator 544 (if present), pattern matching engine 524 (if present), and real-time clock 528 (if present). Enhanced switch 2663 may also act as an interpreter of control signals received from microprocessor 2652 indicating entry to, exit from, and control of SPU mode. z. Switch 2663 in this example recognizes a specific indication (e.g., an instruction fetch access to a designated address in the secure memory 532) as the equivalent to the 'enable `SPU' mode' instruction. Upon recognizing such an indication, it may isolate the CPU/SPU 2650 from external buses and interfaces 2664, 2665, and 2667 such that any external activity, such as DMA cycles, would be 'held' until the switch 2663 permits access again. After this, switch 2663 permits a single access to a specific location in secure memory 532 to complete. aa. The single instruction fetched from the designated location performs a control operation (a cache flush, for example), that can only be performed in microprocessor 2652's most privileged operating mode, and that has an effect visible to switch 2663. Switch 2663 awaits the occurrence of this event, and if it does not occur within the expected number of cycles, does not enter 'SPU' mode. bb. Occurrence of the control operation demonstrates that

	Claim Term/Phrase	Evidence Supporting MS Construction
		microprocessor 2652 is executing in its most privileged 'normal' mode and therefore can be trusted to execute successfully the 'enter `SPU` mode' sequence of instructions stored in secure memory 532. If microprocessor 2652 were not executing in its most privileged mode, there would be no assurance that those instructions would execute successfully. Because switch 2663 isolates microprocessor 2652 from external signals (e.g., interrupts) until 'SPU' mode is successfully initialized, the entry instructions can be guaranteed to complete successfully. cc. Following the initial instruction, switch 2663 can enter 'partial SPU mode,' in which a restricted area of ROM 532 and RAM 534 may be accessible. Subsequent instructions in secure memory 532 may then be executed by microprocessor 2652 to place it into a known state such that it can perform SPU functions--saving any previous state in the restricted area of RAM 534 that is accessible. After the known state is established, an instruction may be executed to deliver a further indication (e.g., a reference to another designated memory location) to switch 2663, which would enter 'SPU' mode. If this further indication is not received within the expected interval, switch 2663 will not enter 'SPU' mode. Once in 'SPU' mode, switch 2663 permits access to all of ROM 532, RAM 534, and other devices in SPU chip 2660. dd. The instructions executed during 'partial SPU' mode must be carefully selected to ensure that no similar combination of instructions and processor state could result in a control transfer out of the protected SPU code in ROM 532 or RAM 534. For example, internal debugging features of microprocessor 2652 must be disabled to ensure that a malicious program could not set up a breakpoint later within protected SPU code and receive control. Similarly, all address translation must be disabled or reinitialized to ensure that previously created MMU data structures would not permit SPU memory accesses to be compromised. The requirement that the instructions for 'partial SPU mode' run in the microprocessor 2652's most privileged mode is necessary to ensure that all its processor control functions can be effectively disabled. ee. The switch 2663 provides additional protection against tampering by ensuring that the expected control signals occur after an appropriate number of clock cycles. Because the 'partial SPU' initialization sequence is entirely deterministic, it is not feasible for malicious software to interfere with it and still retain the same timing characteristics, even if malicious software is running in microprocessor 2652's most privileged mode. ff. Once in 'SPU' mode, switch 2663 may respond to additional indications or signals generated by microprocessor 2652 (e.g., references to specific memory addresses) controlling features of SPU mode. These might include enabling access to external buses 2664 and 2665 so that SPU-protected code could reference external memory or devices. Any attempts by components outside CPU/SPU 2650 to perform operations

	Claim Term/Phrase	Evidence Supporting MS Construction
		(e.g., accesses to memory, interrupts, or other control functions) may be prevented by switch 2663 unless they had been explicitly enabled by instructions executed after 'SPU' mode is entered. To leave SPU mode and return to normal operation, the instructions executing in 'SPU' mode may provide a specific indication to switch 2663 (e.g., a transfer to a designated memory address). This indication may be recognized by switch 2663 as indicating a return to 'normal mode,' and it may again restrict access to ROM 532, RAM 534, and all other devices within SPU chip 2660, while re-enabling external buses and control lines 2664, 2665, and 2667. The instructions executed subsequently may restore the CPU state to that which was saved on entry to SPU mode, so that microprocessor 2652 may continue to perform functions in progress when the SPU was invoked. gg. In an alternate embodiment, the entry into SPU mode may be conditioned on an indication recognized by switch 2663, but the switch may then use a hardware mechanism (e.g., the processor's RESET signal) to reinitialize microprocessor 2562. In such an embodiment, switch 2663 may not implement partial SPU mode, but may instead enter SPU mode directly and ensure that the address from which instructions would be fetched by microprocessor 2652 (specific to microprocessor 2652's architecture) results in accesses to appropriate locations in the SPU memory 532. This could reduce the complexity of the SPU mode entry mechanisms in switch 2663, but could incur an additional processing cost from using a different reinitialization mechanism for microprocessor 2652. hh. SPU chip 2660 may be customized to operate in conjunction with a particular commercial microprocessor. In this example, the SPU may be customized to contain at least the specialized 'enter SPU mode' instruction sequences to reinitialize the processor's state and, to recognize special indications for SPU control operations. SPU chip 2660 may also be made electrically compatible with microprocessor 2652's external bus interfaces. This compatibility would permit CPU/SPU 2650 to be substituted for microprocessor 2652 without change either to software or hardware elsewhere in a computer system. ii. In other alternate embodiments, the functions described above for SPU chip 2600, microprocessor 2652, and internal buses 2661, 2662, and 2666 could all be combined within a single integrated circuit package, and/or on a single silicon die. This could reduce packaging complexity and/or simplify establishment of the hardware tamper-resistant barrier 502. jj. The hardware configuration of an example of electronic appliance 600 has been described above. The following section describes an example of the software architecture of electronic appliance 600 provided by the preferred embodiment, including the structure and operation of preferred embodiment 'Rights Operating System' ('ROS') 602."

	Claim Term/Phrase	Evidence Supporting MS Construction
		2. See '900 230:55 – 233:34 a. "Integrity of Software-Based PPE Security b. As discussed above in connection with FIG. 10, some applications may use a software-based protected processing environment 650 (such as a 'host event processing environment' (HPE) 655) providing a software-based tamper resistant barrier 674. Software-based tamper resistant barrier 674 may be created by software executing on a general-purpose CPU. Various software protection techniques may be used to construct and/or provide software-based tamper resistant barrier 674. c. The risks or threat of attacks described above in connection with PPE 650 apply to a software-based PPE. An important threat to be countered with respect to a software-based tamper resistant barrier 674 is an attack based on a distributable computer program that can defeat the tamper resistant barrier wherever the program is run. Since a software-based tamper resistant barrier 674 typically will not be as secure as a hardware-based tamper resistant barrier 502, it is useful to explore example steps and procedures a 'cracker' might use to "crack` a software'-based tamper resistant barrier. d. FIGS. 67A and 67B show example 'cracking' techniques a 'cracker' might use to attack software-based tamper resistant barrier 674. e. Referring to FIG. 67A, the software used to create tamper resistant barrier 674 may be distributed, for example, on a storage medium 3370 such as a floppy diskette or optical disk (or, this software could be distributed electronically over network 108 and stored locally in a computer memory). The software distribution medium 3370 provides software (code and data) for loading into a computing device such as a general purpose personal computer 3372, for example. Personal computer 3372 may include, for example, a random access memory 3374 and a hard disk 3376. f. In one example, the software distribution medium 3370 might include installation materials 3470 and operational materials 3472. The installation materials 3470 may be executed by computer 3372 to install the operational materials 3472 onto the computer's hard disk 3376. The computer 3372 may then execute the operational materials 3472 from its hard disk 3376 to provide software-based protected processing environment 650 and associated software-based tamper resistant barrier 672. g. In this example, one attack technique an attacker might use is to analyze software distribution medium 3370 (see FIG. 67B, block 3352). Such analysis can take many forms. h. Such analysis could be performed by a combination of one or more techniques. Such techniques include, but are not limited to, the following: i. An attacker can manually 'dump' and/or disassemble listings of the data from medium 3370. This analysis is represented in FIG. 67A by magnifying glass 3352A. j. An attacker can use cryptoanalytic and/or key search techniques to

	Claim Term/Phrase	Evidence Supporting MS Construction
		decrypt any encrypted data from medium 3370. k. An attacker can use automated or semi-automated disassembly tools to explore the functions of programs stored on medium 3370 by studying the operation and flow of the assembly language representation of the programs. This analysis is represented in FIG. 67A by block 3352B. l. An attacker can use software reverse-engineering tools to reconstruct high-level language representations of the programs on medium 3370, and study their functions. This analysis is represented in FIG. 67A by block 3352C, producing source code 3371. m. An attacker can use software reverse-engineering tools to create an equivalent program to the programs stored on medium 3370. As the equivalent program may be in a more convenient form, possibly in a higher-level language, it may be more amenable to analysis. This analysis is also represented in FIG. 67A by block 3352C, producing source code 3371. n. An attacker can use software debugging and/or simulation tools to follow and/or modify the dynamic execution of programs from medium 3370. This technique can be combined with any of the above static analysis techniques to study the program as it operates. This analysis is represented in FIG. 67A by block 3352B. o. An attacker can use hardware-based debugging and/or simulation tools (e.g., an in-circuit emulator, or ICE) to follow and/or modify the dynamic execution of programs from medium 3370. This technique may be more effective than the equivalent using software debugging and/or simulation tools because it has less potential effect on operation of the programs. This analysis is represented in FIG. 67A by block 3352B. p. Such analysis could provide clues and insights into the installation materials 3470, the operational materials 3472, or both. q. Another attack technique could focus on the operational materials 3472 in the form in which they are installed on personal computer 3372. For example, one form of analysis might involve analyzing the on-disk copy of the installed software and/or associated data files installed on computer hard disk 3376 (see FIG. 67B, block 3354). This analysis is represented in FIG. 67A as a magnifying glass 3354B. Because the installed operational materials 3472 can be executed by computer 3372, the analysis need not be limited to analyzing the static information stored on hard disk 3376, but could involve performing static and/or dynamic analysis of the executing software (see FIG. 67B, blocks 3356, 3358). Any of the techniques described above could be used to analyze the operational material software 3472 to yield source code or other more interpretable form 3373A and/or a memory image 3373B. The static and/or dynamic data within RAM 3374A could be similarly analyzed (see FIG. 67A, magnifying glass 3354A). r. The resulting source code 3373A and/or memory image 3373B could be carefully analyzed and reviewed (see magnifying glasses 3354D, 3354E) to obtain an understanding of both the static and dynamic structure and

	Claim Term/Phrase	Evidence Supporting MS Construction
		operation of operational materials 3272. Dynamic code analysis could involve, for example, tracing, single-stepping, data, or code break points of the executing software image, using analysis techniques such as described above. The executing software could be modified dynamically (for example, by patching) during normal operation to attempt to bypass its protection mechanisms and/or to learn more about how it operates (see FIG. 67B, block 3360, and the 'changes' inserted into FIG. 67A memory image 3373B). s. A further attack technique in this example might involve comparing installed operational material 3472 software and data files among several different PPE 650 instances to identify important data structures, such as cryptographic keys (see 'compare' block 3362A of FIG. 67A; and FIG. 67B, block 3362). The resulting list of differences 3362B could be carefully analyzed (see FIG. 67A's magnifying glass 3362C) to obtain important clues, using analysis techniques such as described above. t. A further attack technique might involve comparing the memory and/or disk images of installed operational material 3472 software and data files in a single instance of PPE 650, after performing various operations using the PPE. This could serve to identify important data structures, such as cryptographic keys (see 'compare' block 3362A of FIG. 67A; and FIG. 67B, block 3362). The resulting list of differences 3362B could be carefully analyzed (see FIG. 67A's magnifying glass 3362C) to obtain important clues, using analysis techniques such as described above. u. A further attack technique might involve analyzing the timing and/or order of modification to memory and/or disk images of installed operational material 3472 software and data files in a single instance of PPE 650, during the performance performing various operations using the PPE. This could serve to identify important data structures, such as cryptographic keys (see 'compare' block 3362A of FIG. 67A; and FIG. 67B, block 3362). The resulting list of differences 3362B could be carefully analyzed (see FIG. 67A's magnifying glass 3362C) to obtain important clues, using analysis techniques such as described above. v. A further attack technique might involve duplicating one installed operational material 3472 instance by copying the programs and data from one personal computer 3372B to another personal computer 3372C or emulator (see FIG. 67B, block 3364, and the 'copy' arrow 3364A in FIG. 67A). The duplicated PPE instance could be used in a variety of ways, such as, for example, to place an impostor PPE 650 instance on-line and/or to permit further dynamic analysis. w. A still additional avenue of attack might involve, for example, saving the state of a PPE 650 (see FIG. 67A, block 3366B)--for example, before the expenditure of credit--and restoring the state at a subsequent time (e.g., after a payment operation occurs) (see FIG. 67A, arrows 3366A, 3366C, and FIG. 67B, block 3366). The stored state information 3366B may also be analyzed (see FIG. 67A, magnifying glass 3354F. x. No software-only tamper resistant barrier 674 can be wholly effective

	Claim Term/Phrase	Evidence Supporting MS Construction
		against all of these threats. A sufficiently powerful dynamic analysis (such as one employing an in-circuit emulator) can lay bare all of the software-based PPE 650's secrets. Nonetheless, various techniques described below in connection with FIG. 69A and following make such an analysis extremely frustrating and time consuming--increasing the 'work factor' to a point where it may become commercially unfeasible to attempt to 'crack' a software-based tamper resistant barrier 674." 3. See '900 235:28 – 244:15 a. "Example Techniques for Forming Software-Based Tamper Resistant Barrier b. Various software protection techniques detailed above in connection with FIG. 10 may provide software-based tamper resistant barrier 674 within a software-only and/or hybrid software/hardware protected processing environment 650. The following is an elaboration on those above-described techniques. These software protection techniques may provide, for example, the following: c. An on-line registration process that results in the creation of a shared secret between the registry and the PPE 650 instance--used by the registry to create content and transactions that are meaningful only to that specific PPE instance. d. An installation program (that may be distinct from the PPE operational material software) that creates a customized installation of the PPE software unique to each PPE instance and/or associated electronic appliance 600. e. Camouflage protections that make it difficult to reverse engineer the PPE 650 operational materials during PPE operation. f. Integrity checks performed during PPE 650 operation (e.g., during on-line interactions with trusted servers) to detect compromise and minimize damage associated with any compromise. g. In general, the software-based tamper resistant barrier 674 may establish 'trust' primarily through uniqueness and complexity. In particular, uniqueness and customization complicate the ability of an attacker to: make multiple PPE instances with the same apparent identity; make it harder for an attacker to create a software program(s) that will defeat the tamper-resistant barrier 674 of multiple PPE instances; make it harder for the attacker to reverse engineer (e.g., based upon encryption so that normal debugging/emulation and other software testing tools can't easily provide access); and make it more difficult for an attacker to compare multiple PPE instances to determine differences between them. h. In addition, the overall software-based tamper resistant barrier 674 and associated PPE system is sufficiently complex so that it is difficult to tamper with a part of it without destroying other aspects of its functionality (i.e., a 'defense in depth'). Camouflaging techniques complicate an attacker's analysis through use of debugging/emulation or other software tools. For example, the PPE 650 may rewrite or overwrite

	Claim Term/Phrase	Evidence Supporting MS Construction
		memory locations immediately after using same to make their contents unavailable for scrutiny. Similarly, the PPE 650 operational software may use hardware and/or time dependent sequences to prevent emulation. Additionally, some of the PPE 650 environment code may be self-modifying. These and other techniques make it much harder to crack an individual PPE 650 instance, and more importantly--much harder to write a program that could be used to defeat security on multiple PPE instances. Because the legitimate owner/user of a particular PPE instance may be trying to attack the security of his own system, these techniques assume that individual instances may eventually be cracked and provide additional security and safeguards that prevent (or make it more difficult) for the attacker who has cracked one PPE instance to use that information successfully in cracking other PPE instances. Specifically, these security techniques make it unlikely that an attacker who has successfully cracked one or a small number of PPE instances can write a program capable of compromising the security of any arbitrary other PPE instance, for example. i. Example Installation Process j. Briefly, the preferred example software-based PPE 650 installation process provides the following security techniques: encrypted software distribution, installation customized on a unique instance and/or electronic appliance basis, encrypted on-disk form, installation tied to payment method, unique software and data layout, and identifiable copies. k. FIG. 69A shows one example technique for distributing the PPE 650 software. In this example, the PPE 650 software is distributed as two separate parts and/or media: the installation materials 3470, and the operational materials 3472. Installation materials 3470 may provide executable code and associated data structures for installing the operational materials 3472 onto a personal computer hard disk 3376, for example (see FIG. 67A). The operational materials 3472 may provide executable code and associated data structures for providing protected processing environment 650 and associated software-based tamper resistant barrier 674. l. In this example, installation materials 3470 and operational materials 3472 are each encrypted by a 'deliverable preparation' process 3474 to provide encrypted installation materials 3470E and encrypted operational materials 3472E (the encrypted portions are indicated in FIG. 69A, by cross-hatching). In this example, a small portion 3470C of the installation materials 3470 may be maintained in clear (unencrypted) form to provide an initial portion of the installation routine that may be executed without decryption. This plain text portion 3470C may, for example, provide an initial dialog, using an encrypted or other secure protocol with a trusted

	Claim Term/Phrase	Evidence Supporting MS Construction
		registry 3476 such as VDE administrator 200h for example. This makes the distributed installation materials 3470 and operational materials 3472 meaningless and unreadable to an attacker without additional information since the entire content (except for the initial dialog with the registry 3476) is unreadable. m. In this example, the 'deliverable preparation' process 3474 may encrypt the installation materials 3470 and operational materials 3472 using one or more secret keys known to the registry 3476. Multiple versions of these installation materials 3470 and operational materials 3472 may be distributed using different, secret keys so that compromise of one key exposes only a subset of the software distribution to unwanted disclosure. The only non-encrypted part of the software distribution in plaintext is that portion 3470C of installation materials 3470 used to establish initial contact with the registry 3476. n. The registry 3476 maintains a copy of the corresponding decryption keys within a key generation and cataloging structure 3478. It provides these keys on demand during the registration process (e.g., using a secure key exchange protocol, for example) to only legitimate users authorized to set up a new protected processing environment 650. o. FIGS. 69B-69C show example steps that may be performed by a installation routine 3470 to install a protected processing environment 650. In this example, upon coupling the installation materials 3470 to an electronic appliance 600 such as a personal computer 3372, the appliance begins executing the unencrypted installation materials portion 3470C. This plain text portion 3470C controls appliance 600 to contact registry 3476 and establish a registry dialog (FIG. 69B, block 3470(1)). The appliance 600 and the registry 3476 use a secure key exchange protocol to exchange installation keys so that the registry may deliver the appropriate installation key to the appliance (FIG. 69B, block 3470(2)). Using the provided installation key(s), the appliance 600 may decrypt and run additional portions of encrypted installation materials 3470E (FIG. 69B, block 3470(3) and following). Based on this additional installation program execution, appliance 600 may decrypt and install encrypted operational materials 3472E (FIG. 69B, block 3470(4)). p. Rather than simply installing the operational materials 3472, in one example, installation materials 3470 makes the installation different for each PPE 650 instance. For example, the installation materials 3470 may customize the installation by: uniquely embedding important data into the installed software, uniquely encrypting the installed software, uniquely making random changes to the installed software, uniquely mating the installed software with a particular electronic appliance 600, providing a unique static and/or dynamic layout or other structure. q. Randomly Embedded Cryptographic Keys r. Installation routine 3470 may, for example, modify the operational

	Claim Term/Phrase	Evidence Supporting MS Construction
		materials 3472 to customize embedded locations where critical data such as cryptographic keys are stored. These keys may be embedded into the text of the operational materials 3472 at locations that vary with each installation. In this example, the registry 3476 may choose, on a random or pseudo-random basis, at least some of the operational material 3472 locations in which a particular installation routine 3470 may embed cryptographic keys or other critical data (see FIG. 69B, block 3470(5)). s. The installation process for the operational software may involve decrypting its distribution (which may be the same for all end users) and modifying it to encode the specific locations where its critical data (e.g., cryptographic keys) are stored. These keys may be embedded within the text of the program at locations that vary with every installation. The distribution of unique information into the operational software 3472 can be based on a secret key known to the registry 3476. This key may be communicated by the registry 3476 during the registration dialog using a secure key exchange. The key is shared between the registry 3476 and the PPE 650 instance, and can serve both to organize the installed PPE software, and as the basis of subsequent integrity checks. t. As shown in FIG. 69D, the operational materials 3472 may include embedded locations 3480(a), 3480(b), 3480(c), 3480(d), 3480(e), ... reserved for storing (embedding) critical information such as cryptographic keys. Each of these locations 3480 may initially store a random number string. In one example, the registry 3476 or installation routine 3470 performs a random operation 3482 to randomly select which subset of these locations 3480 is to be used by a particular instance for storing critical data. This selection list 3484 is applied as an input to an operation materials preparation step 3474a (part of the deliverable preparation operation 3474 shown in FIG. 69A). The operation materials preparation step 3474a also accepts, as an input, cryptographic keys from a secure key store 3486. In this example, the operation materials preparation step 3474a embeds the cryptographic keys provided by key store 3486 into the selected locations 3484 of operation materials 3472. u. In accordance with one example, the random operation 3482 selects a subset that is much less than all of the possible locations 3480--and the locations 3480 not used for storing cryptographic keys store random data instead. An attacker attempting to analyze installed operational materials 3472 won't be able to tell the difference between real cryptographic keys and random number strings inserted into a place where cryptographic keys might be stored. v. In this example, the random location selection 3484 (which is unique for each installation) may itself be encrypted by block 3488 based on an installation-unique key provided by key generation block 3490 for example. The encryption key may be securely maintained at registry 3476 so that the registry may later notify the installation materials 3470 of this key--allowing the installation materials to decrypt the resulting encrypted key location block 3492 and recover listing 3484 of the subset

	Claim Term/Phrase	Evidence Supporting MS Construction
		of locations 3480 used for embedding cryptographic keys. w. Embedded Customized Random Changes x. Referring once again to FIG. 69B, the installed operational materials 3472 may be further customized for each instance by making random changes to reserved, unused portions of the operational materials (FIG. 69B, block 3470(6)). An example of this is shown in FIG. 69E. In this example, the operational materials 3472 include unused, embedded random data or code portions 3494. Another technique with similar effect is shown in FIG. 69F. In this example, false code sections 3496 are included within reserved areas of the operational materials 3472. These false code sections 3496 add complexity, and may also be used as a electronic 'fingerprint' to help trace copies. Because the false code sections 3496 are executable program code that are never executed (or if executed perform no actual functions other than confounding analysis by, for example, creating, modifying and/or destroying data that has no impact on the operation of PPE 650 but may appear to have such an impact), they can be used to confound analysis because they may be difficult for an attacker to distinguish from true code sections. In addition other false code may have the effect of disabling the execution of PPE 650 if executed. Correspondence Between Installed Software and Appliance 'Signature'. Another technique that may be used during the installation routine 3470 is to customize the operational materials 3472 by embedding a 'machine signature' into the operational materials to establish a correspondence between the installed software on a particular electronic appliance 600 (FIG. 69C, block 3470(7)). This technique prevents a software-based PPE 650 from being transferred from one electronic appliance 600 to another (except through the use of the appropriate secure, verified backup mechanism). y. For electronic appliances 600 where it is feasible to do so, the installation procedure 3470 may determine unique information about the electronic appliance 600 (e.g., a 'signature' SIG in the sense of a unique value--not necessarily a 'digital signature' in the cryptographic sense). Installation routine 3470 embeds the electronic appliance 'signature' SIG in the installed operational materials 3472. Upon initialization, the operational materials 3472 validate the embedded signature value against the actual electronic appliance 600 signature SIG, and may refuse to start if the comparison fails. z. Depending on the configuration of electronic appliance 600, the machine signature may consist, for example, of some combination of a hash of the ROM BIOS 658' (see FIG. 69G), a hash of a disk defect map 3497a, the Ethernet (or other) network adapter 666 address, information written into an unused disk sector, information stored in a non-volatile CMOS RAM(such as used for hardware configuration data), information stored in non-volatile ('flash') memory (such as used for system or peripheral component 'BIOS' programs) and/or hidden unique information placed into the root directory 3497b of the fixed disk drive 668.

	Claim Term/Phrase	Evidence Supporting MS Construction
		aa. FIG. 69G shows an example of some of these appliance-specific signatures. bb. In this example, machine signature information need not be particularly large. Security is provided by hiding the machine signature rather than on any other cryptographic strength, because there is no more secure mechanism for key storage to protect it. Thus, it is satisfactory for the signature to be just large enough (e.g., two bytes) that it is unlikely to be duplicated by chance. cc. For some electronic appliances 600 where it can be determined that the technique is safe, an otherwise unused section of the non-volatile CMOS RAM 656a may be used to store a signature 3497d. Signature 3497d is verified against the PPE 650's internal state whenever the PPE is initialized. Signature 3497d may also be updated whenever a significant change is made to the secure database 610. If the CMOS RAM signature 3497d does not match the database value, PPE 650 may take this mismatch as an indication that a previous instance of the secure database 610 and/or PPE 650 software has been restored, and appropriate action can be taken. This mechanism thus ensures that even a bit-for-bit copy of the system's fixed disk 668 or other storage medium cannot be saved and reloaded to restore an earlier PPE 650 state. This particular technique depends upon there being an unused location available within CMOS RAM 656a, and may also require the CMOS RAM checksum algorithm to be known. An incorrect implementation could cause a subsequent reboot of electronic appliance 600 to fail because of a bad CMOS checksum, or worse, could alter some critical configuration parameter within CMOS RAM 656a so that electronic appliance 600 could not be recovered. Thus, care must be taken before modifying the contents of CMOS RAM 656a. dd. A still alternate technique may involve marking otherwise 'good' disk sectors 3497c defective and using the sector(s) to store machine signatures and/or encryption keys. This technique ensures that a logical bit-for-bit copy of the media does not result in a usable PPE 650 instance, and also provides relatively inaccessible and non-volatile storage for the information. Because a relatively large amount of storage space can be reserved using this technique, there is enough storage for a cryptographically strong value. ee. Some of the 'machine signature' techniques discussed above may be problematic in some electronic appliances 600 because it may be difficult to locate appropriate appliance-unique information. For example, although in a personal computer a ROM BIOS 658' is always available, the ROM BIOS information by itself may be insufficient because it is likely to be identical for a batch of electronic appliances 600 purchased together. Identifying a network adapter 666 and determining its address is potentially difficult due to the wide variety of adapters; additionally, an electronic appliance's network address may change (although this occurrence may be infrequent). Inserting random signature values into unused bytes within the fixed disk root directory 3497b and/or partition

	Claim Term/Phrase	Evidence Supporting MS Construction
		records may trigger some virus-checking programs, and the data may be modified by defragmentation or other disk manipulation programs. Where supported, a truly unused disk sector 3497c (e.g., one that is marked 'bad' even though it may still viably store information) may be used to store the machine signature. Even so, normal maintenance, upgrades or other failure recovery procedures may disrupt a particular machine association. Since the VDE administrator 200h participates in restoring a PPE 650 based on an encrypted backup image (as described above for example in connection with FIGS. 39-40), the VDE administrator may establish new associations at this point to maintain correspondence between a particular PPE 650 installation and a particular electronic appliance 600. ff. Tie Installation to Payment Method gg. A still additional example technique for providing additional security is to tie a particular PPE 650 installation at registration time to a particular payment method (see FIG. 69C, block 3470(8)). The registration process at installation time may thus serve to tie the PPE 650 installation to some payment method associated with the user, and to store the payment association information both within the PPE 650 instance and at the registry 3476. This technique assures that the actions of a particular PPE 650 instance are accountable to the assigned user with at least the reliability of whatever payment/credit verification technique is employed. hh. Install Operational Materials in Encrypted Form ii. Operational materials 3472 may first be customized as described above for the particular instance and/or appliance 600, then (at least mostly) encrypted for installation into the appliance such as by storage onto disk 668 (see FIG. 69C, block 3470(9)). Different installations may use different sets of decryption keys to decrypt the information once installed. Different parts of operational materials 3472 may be encrypted with different cryptographic keys to further complicate the analysis. This encryption makes analysis of the on disk form of the operational materials 3472 more difficult or infeasible. jj. The beginning of the resulting stored executable file may contain a small decryption program ('decryptor') that decrypts the remainder of the operational materials 3472 as they are loaded into memory. Confounding algorithms (as described below) may be used in this decryptor to make static recovery of the cryptographic keys difficult. Although the decryptor is necessarily in unencrypted form in an all-software installation without hardware support, the use of confounding algorithms to develop the associated cryptographic keys effectively requires a memory image to be captured after the program has been decrypted. Where supported (as described above), an unused and inaccessible disk sector 3497c may be used to store the decryption keys, and the operational materials 3472 may possess only the address for that particular sector. Embedding this address further complicates analysis. kk. Customized Layout

	Claim Term/Phrase	Evidence Supporting MS Construction
		ll. The installation materials 3470 may store the encrypted operational materials 3472 onto the fixed disk 668 using a customized storage layout (FIG. 69C, block 3470(10)). FIG. 69F, 69H, 69I and 69J shows example customized software and data layouts. In these examples, each installed instance of operational materials 3472 is different in both executable form and in data layout. These modifications make each PPE 650 instance require separate analysis in order to determine the storage locations of its critical data such as cryptographic keys. This technique is an effective counter to creation of programs that can undo the protections of an arbitrary PPE 650 instance. mm. Instruction sequences within the operational materials 3472 may be modified by the installation routine to change the execution flow of the executable operational materials 3472 and to alter the locations at which the software expects to locate critical data. The alterations in program flow may include customization of time-consuming confounding algorithms. The locations of the modifiable instruction sequences may be embedded within operational materials 3470, and may therefore be not directly available from an examination of the installation and/or operational materials. nn. FIG. 69H shows one example operational materials 3472 executable code segment provided distinct processes 3498a, 3498b, 3498c, 3498d, 3498e. In this particular example, segment 3498a is executed first and segment 3498e is executed last, but the processes 3498b, 3498c and 3498d may be performed in any order (i.e., they are sequence independent processes). The installation materials 3470 may take advantage of this sequence independence by storing and/or executing them in different and/or depending upon the particular PPE instance 650. FIG. 69I, for example, shows a first static layout order, and FIG. 69J shows a second, different static layout order. Data elements associated with the executables may similarly be stored in different orders (as shown in FIGS. 69I, 69J) depending upon the particular installation. oo. Dynamic Protection Mechanisms pp. In addition to the more static protection mechanisms described above, dynamic protection mechanisms may be employed to complicate both static and dynamic analysis of the executable (executing) operational materials 3472. Such techniques include, for example: qq. implementation complexity, immediate overwriting, hardware dependent sequences, timing dependencies, confounding algorithms, random modifications, dynamic load module decryption, rr. on-line integrity checks, time integrity checks, machine association integrity checks, dynamic storage integrity checks, and hidden secret storage volatile secret storage internal consistency checks. ss. FIGS. 69K-69L show an example execution of operational materials 3472 that may employ some or all of these various dynamic protection mechanisms. tt. Upon starting execution (FIG. 69K, block 3550), the installed operational

	Claim Term/Phrase	Evidence Supporting MS Construction
		materials 3472 may run initialization code as described above that is used to decrypt the stored encrypted operational materials on an 'as needed' basis (FIG. 69K, block 3552). This initialization code may also check the current value of the real-time clock (FIG. 69K, block 3554). uu. Real Time Check/Validation vv. Operational materials 3472 may perform this time check, for example, to guard against replay attacks and to ensure that the electronic appliance 600's time is in reasonable agreement with that of the VDE administrator 200h or other trusted node. ww. FIG. 69M shows an example sequence of steps that may be performed by the 'check time' block 3554. In this example, PPE 650 uses secure communications (e.g. a cryptographic protocol) to obtain the current real time from a trusted server (FIG. 69M, block 3554a). PPE 650 may next ask the user if he or she wishes to reset the electronic appliance real-time clock 528 (which may, for example, be the real-time clock module within a personal computer or the like) so it is synchronized with the trusted server's time clock. xx. If the user responds affirmatively, PPE 650 may reset the time clock to agree with the real-time provided by the trusted server ('yes' exit to decision block 3554b, FIG. 69M, block 3554c). If the user responds that he or she does not want the real-time clock reset ('no' exit to decision block 3554b), then PPE 650 may calculate a delta value of the difference between the server's real-time clock and the electronic appliance's real-time clock 528 (FIG. 69M, block 3554d). In either case, PPE 650 may store the current time Tcurrent into a non-volatile storage location Tstore indicating the current real-time (FIG. 69M, block 3554e). yy. Referring again to FIG. 69K, PPE 650 can disable itself if there is too much (or the wrong type) of a difference between the trusted server's time and the electronic appliance's clock--since such differences can indicate replay attacks, the possibility that the PPE 650 has been restored based on a previous state, etc. For example, if desired, PPE 650 can generate a time check fail exception if the electronic appliance's real-time clock 528 disagrees with the trusted server's real-time by more than a certain amount of acceptable drift (FIG. 69K, 'yes' exit to decision block 3556). In the event of such an exception, PPE 650 may disable itself (FIG. 69K, block 3558) and require a dialog between the user and registry 3476 (or other authority)--providing additional protection against replay attacks and also detecting clock failures that could lead to incorrect operation or incorrect charges. zz. Dynamic Code Decryption and Data OverWriting aaa. Operational materials 3472 may then decrypt the next program segment dynamically (FIG. 69K, block 3460. The code may be decrypted dynamically when it is needed, then re-encrypted or overwritten and discarded when not in use. This mechanism increases the tamper-resistance of the executable code--thus providing additional tamper resistance for PPE operations. As mentioned above, different decryption

	Claim Term/Phrase	Evidence Supporting MS Construction
		keys may be required to decode different code portions, and the decryption keys can be installation-specific so that an attacker who successfully comprises the decryption key of one instance cannot use that information to compromise any other instance's decryption key(s). bbb. Once a portion of the operational materials 3472 has been decrypted (FIG. 69K, block 3560), that portion may immediately overwrite all initialization code in memory since it is no longer required (FIG. 69K, block 3562). The executing operational materials 3472 may similarly overwrite all unwrapped cryptographic keys once they are no longer needed, and may also overwrite expanded key information developed by initializing the cryptographic algorithms once no longer needed. These techniques minimize the amount of time during which usable key information is available for exposure in a memory snapshot--complicating all but the most dynamic of analysis efforts. Because all keys in permanent storage are either encrypted or otherwise camouflaged, no such treatment is required for I/O buffers. ccc. Dynamic Check of Association Between Appliance and PPE Instance ddd. The executing operational materials 3472 may next compare an embedded electronic appliance signature SIG' against the electronic appliance signature SIG stored in the electronic appliance itself (FIG. 69K, decision block 3564). As discussed above, this technique may be used to help prevent operational materials 3472 from operating on any electronic appliance 600 other than the one it was initially installed on. PPE 650 may disable operation if this machine signature check fails ('no' exit to decision block 3564, FIG. 69K; disable block 3566). eee. Self-Modifying and/or Hardware-Dependent Code Sequences fff. Executing operational materials 3472 may also employ self-modifying code sequences that cannot easily be emulated with a software debugger or single-stepping program (FIG. 69K, block 3568). These sequences may, for example, be dependent on specific models of electronic appliances 600, and may be patched into the operational materials 3472 as appropriate to installation materials 3470 based on tests performed during the installation process. Such hardware-dependent sequences may be used to ensure that critical algorithms yield different results when executed on the proper hardware as opposed to when executed on different hardware or under software control such as in a debugger or emulator. To prevent such hardware-dependent sequences from being readily recognizable from a static examination of the code, the sequences may be constructed at run time and then invoked so that they can be identified only by analysis of the instruction sequences actually executed. ggg. Dynamic Timing Checks hhh. Executing operational materials 3472 may also make dynamic timing checks on various code sequences, and refuse to operate if they do not execute within the expected interval (FIG. 69K, block 3570, decision block 3572, 'disable' block 3574). An incorrect execution time suggests that the operational materials 3472 are being externally manipulated

	Claim Term/Phrase	Evidence Supporting MS Construction
		and/or analyzed or traced in some manner (e.g., by a software emulator). This technique thus provides additional protection against dynamic analysis and/or modification. iii. The expected execution intervals associated with certain code sequences may be calculated during the installation procedure. Resulting test values may be embedded into the operational materials 3472. These timing tests may be integrated with time integrity tests and dynamic integrity checks to make it more difficult to bypass them simply by patching out the timing check. Care should be taken to eliminate false alarms due to concurrent system activity (e.g., other tasks and/or windows)." ('900 235:28 - 244:15) 4. See also '900 Figs. 69A-N
30.	912.8: "identifying at least one aspect of an execution space required for use and/or execution of the load module"	**Intrinsic:** 1. "For each site, the manufacturer generates a site ID 2821 and list of site characteristics 2822." ('193 209:55-57)

Appendix 1 to Exhibit D: Source Abbreviations

Intrinsic Evidence:

Abbreviated Reference	Full Citation or Title
'193	U.S. Patent No. 6,253,193
'683	U.S. Patent No. 6,185,683
'721	U.S. Patent No. 6,157,721
'861	U.S. Patent No. 5,920,861
'891	U.S. Patent No. 5,982,891
'900	U.S. Patent No. 5,892,900
'912	U.S. Patent No. 5,917,912
'712	U.S. Patent Application Serial No. 08/699,712
'107	U.S. Patent Application Serial No. 08/388,107

Extrinsic Evidence:

Abbreviated Reference	Full Citation or Title
Bishop	M. Bishop, Computer Security, Art & Science, (2003).
Booth	C. J. Booth, ed. The New IEEE Standard Dictionary of Electrical and Electronics Terms, 5th edition, (1993).
Davies	D.W. Davies and W.L. Price, Security for Computer Networks, (1984) MSI083423-MIS083443.
Denning	D. Denning, Cryptography and Data Security, (1983), MSI085569.
Dictionary of Computing	Dictionary of Computing, 3rd edition, Oxford University Press, (1990).
IBM	G. McDaniel, ed., IBM Dictionary of Computing, (1994).
Laplante	P. A. Laplante, ed., Dictionary of Computer Science, Engineering, and Technology (2001).
Longley	D. Longley, et al., Information Security: Dictionary of Concepts, Standards and Terms, (1992).
Neumann	P.G. Neumann, Computer Related Risks, (1995).
Pfleeger	C. P. Pfleeger, Security in Computing, (1989).
Que	C. Weisert, Que's Computer Programmer's Dictionary, (1993).
Russell	D. Russell and G.T. Gangemi, Computer Security Basics, (1991).
Webster's	D. Spencer, Webster's New World Dictionary of Computer Terms, 4th edition (1992).

Exhibit E

Microsoft's Statement of Reservations

Microsoft provides its attached claim construction for each of the 30 "Mini-Markman" terms and phrases, subject to the limitations and reservations of rights set forth herein.

Claim Invalidity: Microsoft does not waive any defenses that the asserted claims fail to satisfy the provisions of 35 U.S.C. § 112, including, for example, the written description requirement, the definiteness requirement, or any other requirement for patentability. Microsoft does not concede that the asserted claims are supported by Plaintiffs original "big book" application or any application from which they purportedly claim priority. By offering a construction of a term, Microsoft does not waive any defense that the claim is indefinite and there can be no proper construction.

Continuing Discovery: Microsoft reserves the right to modify its claim constructions in light of ongoing claim construction discovery, in particular such discovery compelled by Judge James' Order of March 10, 2003. Microsoft reserves the right to modify or supplement its cited extrinsic evidence in light of information that is provided in continuing discovery on claim construction and indefiniteness.

Intrinsic Evidence: For the purposes of submission of this claim construction only, Microsoft treats the "intrinsic" evidence as including: 1) the specifications of each of the seven U.S. patents at issue in the "Mini-Markman" proceeding, including any material purportedly incorporated by reference therein; 2) the prosecution history of each of the seven patents at issue, including the applications and prosecution history of the seven patents and any related patent applications, including without limitation, applications purportedly incorporated by reference or to which an application claimed priority; and 3) all references cited in the prosecution of any such applications. Microsoft does so without waiving the right to contest whether some of this information is or is not properly part of the intrinsic evidence.

Dr. Reiter is expected to testify as follows:

1. Dr. Reiter will testify regarding the meaning of the disputed claim elements to one of ordinary skill in the art, taking into account the understood meaning of the terms in the art, the patent specifications and the file histories. He will testify as follows:

a. InterTrust's proposed definitions, attached as Exhibit B to the Joint Claim Construction Statement ("JCCS") are consistent with the use of the terms or phrases in the specification and the relevant art. Those definitions are attached hereto. Citations to supporting specification text and relevant art can be found in Exhibit C to the JCCS.

b. Microsoft has made repeated substantial changes to its proposed definitions, the changes continuing up to shortly before the present document was prepared. For this reason, it is impossible to include detailed responses to the issues raised by those definitions.

In general, however, the Microsoft definitions incorporate restrictions that are inconsistent with specification use of the terms and/or inconsistent with the understanding of the terms in the art. Those inconsistencies are demonstrated by the attached supporting evidence. The following discussion lists one or more serious deficiencies in each Microsoft definition, but is not intended as a comprehensive description of all such deficiencies.

Individual terms

Access/Access to/Accessing/Accessed

The first sentence of Microsoft's definition is generally consistent with the InterTrust definition. The second sentence of the Microsoft definition is based on a specific disclosed embodiment, and is inconsistent with general use of the term in the specifications.

Addressing

The two parties' definitions are very close. Microsoft's definition is, however, improper in its apparent exclusion of indirect addressing.

Allowing, allows

Microsoft's definition is based on a specific disclosed embodiment and ignores other embodiments. See InterTrust's supporting evidence.

Arrangement

Microsoft's definition requires particular types of organizations and is therefore inconsistent with the patent specifications.

Aspect

Microsoft's definition is overly restrictive in its requirement that an aspect be "persistent" and that it "can be used to distinguish [an environment] from other environments."

Associated with

Microsoft's definition incorporates restrictions based on a particular embodiment and is inconsistent with other disclosed embodiments and with the general meaning of the term.

Authentication

Microsoft's definition requires multiple types of authentication, in a manner not required by use of this term in the specification or the art. Moreover, some of these types cannot be applied (e.g., "origin integrity" applied to an organization).

Authorization information, Authorized, Not authorized

Microsoft's definitions are based on specific embodiments and contradicted by alternative embodiments disclosed in the specifications.

Budget control; Budget

Microsoft's definition improperly restricts "budget" to a particular type of method, and improperly restricts Budget Control in a manner inconsistent with the specification.

Can be

Microsoft's definition incorporates the language "which otherwise cannot be carried out." This language is inconsistent with the specifications.

Capacity

The Microsoft definition relates to hardware storage devices, a context that is irrelevant to use of the term in the relevant claim.

Clearinghouse

Microsoft's definition is inconsistent with use of this term in the specifications. See InterTrust's supporting evidence.

Compares; Comparison

Microsoft's definition is based on a particular type of processor operation, a context that is not discussed in the specification and not required by the claim.

Component assembly

Microsoft's definition incorporates a large number of restrictions based on specific embodiments and ignoring alternate embodiments.

Contain, contained, containing

Microsoft's definition requires "physically" or "directly" storing, and distinguishes Addressing. This is inconsistent with use of the term in the specification.

Control (n.); Controls (n.)

The Microsoft definition incorporates a large number of restrictions based on specific embodiments, and ignores alternate embodiments described in the specifications.

Controlling; Control (v.)

The Microsoft definition incorporates limitations that are not required by the specification, including limitations contradicted by use of the term in the specifications and by disclosed embodiments.

Copied file

The Microsoft definition improperly distinguishes "copied file" from "copy."

Copy, copied, copying (v.)

The Microsoft definition is internally inconsistent, since it both prohibits and allows changes in the reproduced file. That definition also incorporates examples that are inconsistent with use of the terms in the claims.

Copy control

The Microsoft definition is inconsistent with use of this term in the claim.

Data item

The Microsoft definition incorporates limitations not present in the InterTrust definition. These limitations are not required by the specification or normal use of the term in the art.

Derive, Derives

The Microsoft definition requires retrieval, a concept not required by the specifications or use of this term in the claim.

Descriptive data structure

Limitations in the last two sentences of the Microsoft definition are inconsistent with described embodiments and are not required by the specifications or use of the term in the claims.

Designating

The Microsoft definition does not apply to this term, but instead to the claim phrase in which the term is found. That claim phrase is separately defined.

Device class

The Microsoft definition is inconsistent with the definition given to this term during prosecution.

Digital file

The Microsoft definition is overly restrictive. The limitations is incorporates are not required by the specification, use of the term in the claims or general use in the relevant art.

Digital signature; Digitally signing

The Microsoft definition of digital signature requires that the string be "computationally unforgeable," a characteristic that is impossible to obtain. The Microsoft definition of digitally signing requires a secret key, and also includes significant background discussion not necessary for the definition.

Entity's control

Microsoft's definition improperly requires control of a "particular use of or access to particular protected information by a particular user(s)." No such requirements are imposed by the term, the claim or the specifications.

Environment

Microsoft does not appear to have provided any definition for this term.

Executable programming; Executable

Microsoft's requirement of "machine code instructions" is inconsistent with use of this term in the specifications. In addition, Microsoft's definition of "computer program" imposes limitations not required by these terms.

Execution space; Execution space identifier

Microsoft's definition of Execution Space is inconsistent with the explicit definition given to this term during prosecution. Microsoft's definition of Execution Space Identifier improperly requires "unique" identification.

Governed item

Microsoft's definition of Governed Item requires arbitrarily fine granularity and control of "access and use by any user, process, or device." Neither the term nor the specifications require such limitations.

Halting

The Microsoft definition requires execution be "unconditionally" stopped. The specification imposes no such requirement, and the Microsoft definition appears to be based on a particular type of instruction that is not mentioned in the patents.

Host processing environment

The Microsoft definition incorporates the term "VDE node," a term that is itself defined at great length, incorporating numerous improper limitations. The Microsoft definition also improperly incorporates restrictions based on privileged mode versus user mode, and "loaded" software. In addition, the Microsoft definition improperly excludes hardware.

Identifier, Identify, Identifying

The Microsoft definitions improperly restrict these terms to "particular instances."

Including

The definitions are consistent, except that the hardware portion of Microsoft's definition requires "physically present within." This is inconsistent with use of the term in the claims.

Information previously stored

Microsoft's definition would render the claim nonsensical, since it would require a comparison involving information that is no longer available for the comparison.

Integrity programming

The Microsoft definition is internally inconsistent, improperly incorporates the term Executable Programming and improperly defines integrity as excluding all alterations.

Key

Microsoft's exclusion of "key seed or other information from which the actual encryption and/or decryption key is constructed, derived, or otherwise identified" is inconsistent with the specification and general use of the term in the relevant art.

Load module

Microsoft's definition imposes numerous limitations beyond those identified in the InterTrust definition. Those additional limitations are not required by the term and are inconsistent with embodiments disclosed in the specifications.

Machine check programming

The Microsoft definition improperly requires Executable Programming and a "unique 'machine signature' which distinguishes the physical machine from all other machines." These limitations are not required by the term.

Opening secure containers

The Microsoft definition improperly distinguishes "opening" from decrypting, and improperly incorporates limitations based on a particular embodiment of opening.

Operating environment

See Processing Environment.

Organization, Organization information, Organize

The Microsoft definitions improperly incorporate concepts related to physical storage.

Portion

The Microsoft definition improperly implies that presence of a "portion" excludes presence of the whole.

Prevents

The Microsoft definition requires a level of certainty that is inconsistent with the specification and impossible to obtain.

Processing Environment

The Microsoft definition incorporates a specific embodiment and would exclude other embodiments disclosed for this term.

Protected processing environment

The Microsoft definition incorporates at least several dozen highly restrictive and unnecessary limitations, and appears to combine restrictions from multiple separate embodiments.

Protecting

The incorporation of Security into the Microsoft definition is improper, since that term is considerably more general than the manner in which Protecting is used in the claim.

Record

The Microsoft definition includes limitations beyond those incorporated in the InterTrust definition. These added limitations are not required by use of this term in the claims, specification, or art.

Required

The Microsoft definition implies a degree of absoluteness that is inconsistent with the specification. The second sentence of the Microsoft definition is unsupported by the specification or normal use of the term.

Resource processed

The Microsoft definition improperly requires a "shared facility," and that the resource be "required by a job or task." These are not required by the claim or specification.

Rule

The Microsoft definition improperly distinguishes Rules from Controls, and imposes an unsupported requirement that a Rule be a "lexical statement."

Secure

The Microsoft definition requires absolute protection against all possible threats, and is therefore inconsistent with use of the term in the specification, the claims, and the relevant art.

Secure container

The requirements imposed by the Microsoft definition are either inconsistent with the specification or ignore disclosed embodiments.

Secure container governed item

The Microsoft definition imposes a requirement of absolute security that is inconsistent with the specification and ignores alternate disclosed embodiments.

Secure database

The Microsoft definition improperly defines "database" in accordance with one particular type of database, and improperly imposes a requirement of absolute security that is inconsistent with the specification.

Secure execution space

The Microsoft definition is inconsistent with and excludes embodiments of Secure Execution Spaces described in the specification.

Secure memory

Microsoft's definition of "memory" improperly excludes virtual memory. Microsoft's definition of Secure Memory includes numerous restrictions not supported by the specification.

Secure operating environment, Said operating environment

See Secure Processing Environment.

Securely applying

Microsoft's definition of "securely" is inconsistent with and excludes embodiments described in the specification.

Microsoft's definition of Securely Applying improperly includes limitations from specific embodiments, as well as limitations not required by the specification or claims.

Securely assembling

The Microsoft definition incorporates limitations from specific embodiments, and ignores alternate embodiments not requiring those limitations.

Securely processing

The Microsoft definition improperly incorporates a requirement of a secure execution space. This requirement is inconsistent with embodiments described in the specification.

Securely receiving

The Microsoft definition is based on limitations taken from a particular embodiment and ignores alternate embodiments.

Security level, Level of security

The Microsoft definition improperly requires an "ordered measure" and persistence. The second and third sentences from the Microsoft definition are unsupported by any disclosure in the specifications.

Tamper resistance

The Microsoft definition improperly requires a tamper resistant barrier.

Tamper resistant barrier

The Microsoft definition describes a specific embodiment, and is inconsistent with alternate embodiments described in the specifications.

Tamper resistant software

The Microsoft definition improperly requires a tamper resistant barrier.

Use

The second sentence of the Microsoft definition improperly incorporates limitations from a particular embodiment.

User controls

The Microsoft definition is inconsistent with the claim and the prosecution history.

Validity

The Microsoft definition improperly incorporates the concept of "authentication," and applies only to data.

Virtual distribution environment

See Global Construction of VDE.

Claim phrases

193.1

receiving a digital file including music

The Microsoft definition includes numerous unnecessary limitations, including secure container, authentication a recipient and use of controls.

a budget specifying the number of copies which can be made of said digital file

The Microsoft definition improperly includes "copies" that are not "long-lived, decrypted or accessible." The Microsoft definition also ignores embodiments involving alternative control structures.

controlling the copies made of said digital file

The Microsoft definition improperly incorporates limitations from particular embodiments, ignores embodiments describing alternative control structures and imposes numerous limitations that are not supported by the specification or claim language.

determining whether said digital file may be copied and stored on a second device based on at least said copy control

The Microsoft definition incorporates numerous unnecessary limitations not required by the claim or the specification, improperly requires that "the" file, as opposed to a copy, be stored on a second device, excludes described alternative embodiments and requires an absolute degree of control that is inconsistent with the specification.

if said copy control allows at least a portion of said digital file to be copied and stored on a second device

The Microsoft definition's "explanation" of the branches makes no sense and is unsupported by the claim and , improperly requires that "the" file, as opposed to a copy, be stored on a second device.

copying at least a portion of said digital file

The Microsoft definition improperly distinguishes a "copy" and "the" file, and improperly excludes embodiments described in the specification.

transferring at least a portion of said digital file to a second device

The Microsoft definition improperly distinguishes a "copy" and "the" file, improperly requires that controls be executed and ignores alternative embodiments described in the specification.

storing said digital file

The Microsoft definition improperly distinguishes a "copy" and "the" file, and improperly requires storage of the entire file rather than a portion.

193.11

receiving a digital file

The Microsoft definition includes numerous unnecessary limitations, including secure container, authentication a recipient and use of controls.

determining whether said digital file may be copied and stored on a second device based on said first control

The Microsoft definition incorporates numerous unnecessary limitations not required by the claim or the specification, improperly requires that "the" file, as opposed to a copy, be stored on a second device, excludes described alternative embodiments and requires an absolute degree of control that is inconsistent with the specification.

identifying said second device

The Microsoft definition improperly requires that the identification distinguish the device from all other devices, that controls be used and that a VDE Secure Processing Environment be used.

whether said first control allows transfer of said copied file to said second device

The Microsoft definition improperly distinguishes a "copy" from "the" file, and ignores embodiments describing alternative control structures.

said determination based at least in part on the features present at the device

The Microsoft definition improperly requires that all features be used, that these be "actual, current" features and improperly excludes device identifiers.

if said first control allows at least a portion of said digital file to be copied and stored on a second device

The Microsoft definition's "explanation" of the branches makes no sense and is unsupported by the claim and , improperly requires that "the" file, as opposed to a copy, be stored on a second device.

copying at least a portion of said digital file

The Microsoft definition improperly distinguishes a "copy" and "the" file, and improperly excludes embodiments described in the specification.

transferring at least a portion of said digital file to a second device

The Microsoft definition improperly distinguishes a "copy" and "the" file, improperly requires that controls be executed and ignores alternative embodiments described in the specification.

storing said digital file

The Microsoft definition improperly distinguishes a "copy" and "the" file, and improperly requires storage of the entire file rather than a portion.

193.15

receiving a digital file

The Microsoft definition includes numerous unnecessary limitations, including secure container, authentication a recipient and use of controls, and the requirement that the step must proceed in both authentication branches is not supported in the claim.

an authentication step comprising:

The Microsoft definition improperly includes a requirement of an absence of trust, VDE controls and a VDE Secure Processing Environment.

accessing at least one identifier associated with a first device or with a user of said first device

The Microsoft definition improperly requires "securely" accessing, that an identifier identify a "single" user or device (but not "and"), VDE controls, and a VDE Secure Processing Environment.

determining whether said identifier is associated with a device and/or user authorized to store said digital file

The Microsoft definition improperly requires VDE controls and a VDE Secure Processing Environment.

storing said digital file in a first secure memory of said first device, but only if said device and/or user is so authorized, but not proceeding with said storing if said device and/or user is not authorized

The Microsoft definition ignores embodiments describing alternative control structures, and improperly requires that "the" file be stored, as opposed to a copy, VDE controls, and a VDE Secure Processing Environment.

storing information associated with said digital file in a secure database stored on said first device, said information including at least one control

Microsoft's definition improperly requires that the stored information be associated with the digital file but not the digital file's contents, VDE controls, a VDE Secure Processing Environment and that the step proceed regardless of the outcome of the authentication step.

determining whether said digital file may be copied and stored on a second device based on said at least one control

The Microsoft definition incorporates numerous unnecessary limitations not required by the claim or the specification, improperly requires that "the" file, as opposed to a copy, be stored on a second device, excludes described alternative embodiments, requires an absolute degree of control that is inconsistent with the specification, and requires that the step proceed regardless of the outcome of the authentication step.

if said at least one control allows at least a portion of said digital file to be copied and stored on a second device,

The Microsoft definition's "explanation" of the branches makes no sense and is unsupported by the claim and , improperly requires that "the" file, as opposed to a copy, be stored on a second device.

copying at least a portion of said digital file

The Microsoft definition improperly distinguishes a "copy" and "the" file, and improperly excludes embodiments described in the specification and improperly requires that the step proceed regardless of the outcome of the authentication step.

transferring at least a portion of said digital file to a second device

The Microsoft definition improperly distinguishes a "copy" and "the" file, improperly requires that controls be executed and ignores alternative embodiments

described in the specification, and improperly requires that the step proceed regardless of the outcome of the authentication step.

storing said digital file

The Microsoft definition improperly distinguishes a "copy" and "the" file, and improperly requires storage of the entire file rather than a portion, and improperly requires that the step proceed regardless of the outcome of the authentication step.

193.19

receiving a digital file at a first device

The Microsoft definition includes numerous unnecessary limitations, including secure container, authentication a recipient and use of controls.

establishing communication between said first device and a clearinghouse located at a location remote from said first device

The Microsoft definition improperly requires a communications channel and that the communications channel was "previously non-existent."

using said authorization information to gain access to or make at least one use of said first digital file

The Microsoft definition improperly requires that "all of" the authorization information be used, VDE controls, a VDE Secure Processing Environment, and ignores embodiments describing alternative control structures.

receiving a first control from said clearinghouse at said first device

The Microsoft definition includes numerous unnecessary limitations, including secure container, authentication a recipient and use of controls.

storing said first digital file in a memory of said first device

The Microsoft definition improperly requires VDE controls and a VDE Secure Processing Environment.

using said first control to determine whether said first digital file may be copied and stored on a second device

The Microsoft definition incorporates numerous unnecessary limitations not required by the claim or the specification, improperly requires that "the" file, as opposed

to a copy, be stored on a second device, excludes described alternative embodiments and requires an absolute degree of control that is inconsistent with the specification.

if said first control allows at least a portion of said first digital file to be copied and stored on a second device

The Microsoft definition's "explanation" of the branches makes no sense and is unsupported by the claim and , improperly requires that "the" file, as opposed to a copy, be stored on a second device.

copying at least a portion of said first digital file

The Microsoft definition improperly distinguishes a "copy" and "the" file, and improperly excludes embodiments described in the specification.

transferring at least a portion of said first digital file to a second device including a memory and an audio and/or video output

The Microsoft definition improperly distinguishes a "copy" and "the" file, improperly requires that controls be executed and ignores alternative embodiments described in the specification.

storing said first digital file portion

Microsoft's definition improperly distinguishes a "copy" and "the" file.

683.2

the first secure container having been received from a second apparatus

Microsoft's definition improperly requires that the first secure container identify the apparatus from which it was received, and improperly argues that, in the absence of such identification, that container could not be distinguished from a container created at the site. Microsoft's definition includes numerous improper limitations, including authenticating a recipient and authentication occurring in accordance with VDE controls. The examples cited by Microsoft are misleading, since these are specific embodiments rather than general requirements.

an aspect of access to or use of

Microsoft's definition improperly excludes rules governing more than one aspect, improperly excludes access and use and improperly requires that the aspect be governed in relation to "any and all processes, users, and devices."

the first secure container rule having been received from a third apparatus different from said second apparatus

Microsoft's definition improperly requires that the first secure container identify the apparatus from which it was received, and improperly argues that, in the absence of such identification, that container could not be distinguished from a container created at the site. Microsoft's definition includes numerous improper limitations, including receipt in a secure container, authenticating a recipient and authentication occurring in accordance with VDE controls.

hardware or software used for receiving and opening secure containers

Microsoft's definition improperly requires a Secure Processing Environment and SPU, improperly requires "the same single logical piece of either hardware or software (as opposed to both), " and improperly requires authentication and VDE controls.

said secure containers each including the capacity to contain a governed item, a secure container rule being associated with each of said secure containers

The Microsoft definition improperly requires that rules be associated with secure containers, as opposed to governed items.

protected processing environment at least in part protecting information contained in said protected processing environment from tampering by a user of said first apparatus

The Microsoft definition is unsupported in the specification. It is contradicted by the claim and improperly requires numerous elements not required by the specification, including a Secure Processing Environment.

hardware or software used for applying said first secure container rule and a second secure container rule in combination to at least in part govern at least one aspect of access to or use of a governed item contained in a secure container

The Microsoft definition improperly requires a Secure Processing Environment/SPU, a "single" piece of hardware or software, assembly of a control and governance through VDE controls.

hardware or software used for transmission of secure containers to other apparatuses or for the receipt of secure containers from other apparatuses.

The Microsoft definition improperly requires a Secure Processing Environment/SPU, a "single" piece of hardware or software, assembly of a control and governance through VDE controls. The examples cited by Microsoft are misleading, since these are specific embodiments rather than general requirements.

721.1

digitally signing a first load module with a first digital signature designating the first load module for use by a first device class

The Microsoft definition improperly requires that the digital signature be used as the signature key, that all load modules be signed and that certain devices not have keys.

digitally signing a second load module with a second digital signature different from the first digital signature, the second digital signature designating the second load module for use by a second device class having at least one of tamper resistance and security level different from the at least one of tamper resistance and security level of the first device class

The Microsoft definition improperly requires that the digital signature be used as the signature key, that all load modules be signed, that certain devices not have keys, that security levels be persistent and that security levels be greater or less than other security levels.

distributing the first load module for use by at least one device in the first device class

The Microsoft definition improperly requires transmission and that the digital signature accompany the first load module as distributed.

distributing the second load module for use by at least one device in the second device class

The Microsoft definition improperly requires transmission and that the digital signature accompany the first load module as distributed.

721.34

arrangement within the first tamper resistant barrier

The Microsoft definition improperly requires that the arrangement be "executed wholly within the first tamper resistant barrier."

prevents the first secure execution space from executing the same executable accessed by a second secure execution space having a second tamper resistant barrier with a second security level different from the first security level

The Microsoft definition improperly requires that the second secure execution space be part of the protected processing environment, that security level differences be persistent and higher or lower than each other and that the "same" executable be executed.

861.58

creating a first secure container

The Microsoft definition improperly requires a VDE Secure Processing Environment.

including or addressing . . . organization information . . . desired organization of a content section. . . and metadata information at least in part specifying at least one step required or desired in creation of said first secure container

The second paragraph from Microsoft's definition is inconsistent with the claim. The limitations imposed by the third paragraph are not required by the claim or specification.

at least in part determine specific information required to be included in said first secure container contents

The Microsoft definition improperly excludes other reasons for inclusion of the information and improperly requires specific values.

rule designed to control at least one aspect of access to or use of at least a portion of said first secure container contents

The Microsoft definition improperly requires that the rule be designed for particular contents, that the rule be used by VDE controls, the presence of a VDE Secure Processing Environment and that the rule is generated or identified based on the descriptive data structure. Microsoft's definition also excludes embodiments describing alternative control structures.

891.1

resource processed in a secure operating environment at a first appliance

The Microsoft definition improperly requires a shared facility and a Secure Processing Unit with specific features.

securely receiving a first entity's control at said first appliance

The Microsoft definition includes numerous unnecessary limitations, including secure container, authentication, use of controls and encryption on the communications level.

securely receiving a second entity's control at said first appliance

The Microsoft definition includes numerous unnecessary limitations, including secure container, authentication, use of controls and encryption on the communications level.

securely processing a data item at said first appliance, using at least one resource

The Microsoft definition improperly requires a Secure Processing Unit including numerous limitations.

securely applying, at said first appliance through use of said at least one resource said first entity's control and said second entity's control to govern use of said data item

The Microsoft definition improperly requires a Secure Processing Environment consisting of a Secure Processing Unit and that the resource be a component part of a secure operating environment.

900.155

first host processing environment comprising

The Microsoft definition incorporates limitations not required by the claim or the specifications, including limiting the host processing environment to only currently executing software.

designed to be loaded into said main memory and executed by said central processing unit

The Microsoft definition improperly requires that the software is capable of being loaded "only" in the main memory and executed "only" by the CPU.

said tamper resistant software comprising: . . . one or more storage locations storing said information

The Microsoft definition improperly requires that the storage locations be part of the machine check programming and that the storage locations must not store other information.

derives information from one or more aspects of said host processing environment,

The Microsoft definition improperly requires that information be derived from "hardware," and that the information "uniquely and persistently" identify the host processing environment.

one or more storage locations storing said information

The Microsoft definition improperly requires that the storage locations be part of the tamper resistant software and that the storage locations must not store other information.

information previously stored in said one or more storage locations

Microsoft's definition would render the claim nonsensical, since it would require a comparison involving information that is no longer available for the comparison.

generates an indication based on the result of said comparison

Microsoft's definition improperly requires that only two results be possible and that the indication is based solely on the result of the "compares" step.

programming which takes one or more actions based on the state of said indication

The Microsoft definition improperly requires executable programming, that the programming not be part of the host processing environment, that the programming must take an action regardless of the indicator state and that the action must be based solely on the state of the indication.

at least temporarily halting further processing

Microsoft's definition improperly requires that the host processing environment and all processes running in it be halted.

912.8

identifying at least one aspect of an execution space required for use and/or execution of the load module

The Microsoft definition improperly requires that the identifier "define fully, without reference to any other information."

said execution space identifier provides the capability for distinguishing between execution spaces providing a higher level of security and execution spaces providing a lower level of security

The Microsoft definition improperly requires that the execution space identifier provides the load module with the ability to determine a level of security, and the presence of two higher and two lower levels of security.

checking said record for validity prior to performing said executing step

The Microsoft definition improperly requires that the record be checked before execution of any identified information, that evaluation occur within a VDE Secure Processing Environment, and that specific types of information be checked.

912.35

received in a secure container

The Microsoft definition improperly requires "encapsulation" in a secure container, authentication in accordance with VDE controls and acceptance of the secured container.

said component assembly allowing access to or use of specified information

The Microsoft definition improperly requires that the component assembly operate by itself, that it execute in a VDE Secure Processing Environment and that the component assembly be dedicated to specific information. The Microsoft definition ignores embodiments describing alternative control structures and improperly distinguishes access and use.

said first component assembly specified by said first record

The first paragraph of Microsoft's definition defines this term in a restrictive manner with no support in the claim. Microsoft's second paragraph is devoted to a non-existent inconsistency created by Microsoft's restrictive definition.

Claims as a Whole:

In every case, Microsoft requires the system be a VDE or the method be performed in a VDE. This requirement is not supported by the language of any of the claims.

Global Construction

The language of the individual claims contains nothing to support the large number of restrictions imposed by Microsoft's "global construction." Those restrictions are unsupported by and in many cases contradicted by the specification.

2. Digital Rights Management in general. Dr. Reiter will testify regarding Digital Rights Management technology, including encryption and tamper-resistance techniques. The nature and extent of such testimony will depend on the Court's decision as to the scope and format of tutorial presentations.

3. InterTrust's patents and patent claims. Dr. Reiter will testify regarding the general nature of the InterTrust patents, and will summarize the claims at issue in the initial Joint Claim Construction hearing. The nature of that testimony will depend on the

Court's decision as to ordering and format of testimony, but will be consistent with the testimony outlined above regarding claim terms and phrases.

Exhibit G

Summary of Opinions of Professor John Mitchell
<u>In Support of Microsoft's Proposed Claim Constructions</u>

1. In the field of computer security, terms such as "secure," "protect," and "tamper resistance" are understood differently depending on the particular context in which they are used. They have such a range of possible meanings that context is essential to understanding what these terms mean in a given instance. The same is true for terms like "govern" and "control" when they are used to describe computer systems or access to information.

A person skilled in the computer security field would not expect to use a dictionary to understand what these terms mean in a given context; rather, he or she would expect to review the particular reference or system in question to see what adversarial events or attacks are being defended against. Generally speaking, dictionary "definitions" are not sufficient for understanding how these terms are meant in a particular case. A number of terms and phrases used in the February 1995 application (such as "VDE," "PPE," and "secure container") are also not likely to be found in dictionaries.

2. The February 1995 application (which is sometimes referred to as the "Big Book") never clearly explains what it means by "security." It would not be clear to someone of average skill in the field what "secure" means in that application -- for example, with regard to systems, system components, information, or processes. The same is true for such terms as "protected" and "tamper resistant."

3. If a reasonably skillful computer security professional were to presume that "secure" has all of the attributes that are promised in the February 1995 application, then "secure" requires a guarantee of secrecy, authenticity, integrity, nonrepudiation, and availability, against all security threats identified in that application other than excessively costly brute

force attacks. (What constitutes excessive cost in this context is not clearly explained). Again taking the February 1995 application's promises for context, "tamper resistance" requires that some barrier is in place which prevents access to or alteration of information in an unauthorized manner. The terms "secure" and "security", and additional terms such as "secure container," "control," "govern," "protect," "protected processing environment," "host processing environment" and "virtual distribution environment," would be understood, to the extent possible, as set forth in Microsoft's PLR 4-2 Statement, as opposed to the definitions listed in InterTrust's PLR 4-2 Statement.

4. Professor Mitchell will explain the qualifications of a person of reasonable skill in the computer security field, including as of February 13, 1995, and explain how cited references (such as U.S. Patent 5,634,012 to Stefik et al., U.S. Patents 4,868,877 and 5,337,360 to Fischer, Choudhury et al.'s "Copyright Protection for Electronic Publishing over Computer Networks," U.S. Patent 4,658,093 to Hellman, and Mori et al.'s "Superdistribution: The Concept and Architecture" (Transactions of the IECE 1990)) would influence such a person's understanding of the InterTrust disclosure. He may also address the substance of additional references published or created before February 13, 1995, not cited in the InterTrust patents.

5. The specifications of the '721, '900, and '861 patents do not resolve any of these problems with the Big Book application.

Summary of Opinions of Professor David Maier in Support of Microsoft's Proposed Claim Constructions

1. The specification of U.S. Patent No. 6,253,193 ("the '193 patent") describes several mandatory features of the Virtual Distribution Environment ("VDE") architecture, including:

- the creation of a comprehensive data security and commerce world;
- the ability to handle all types of digital works independent of computing platform, making it a single, general purpose solution in contrast to multiple, limited purpose solutions;
- flexible control mechanisms that can be applied to any granularity of content;
- control mechanisms that are configurable by any user, not just the system designers or content providers; and
- isolation of the system programs and protected works from the non-VDE world, preventing observation, alteration, interference, or removal from the VDE, except as permitted by the VDE control mechanisms.

This does not mean that the capabilities of the Virtual Distribution Environment can be achieved, only that these are features that the '193 patent makes clear a VDE must have.

2. The specification of the '193 patent describes a system that requires several architectural elements including at least the following:

- VDE Foundation Hardware and Software – installed throughout an infrastructure of interlinked computing devices;
- The VDE "Secure Container" – a mechanism for packaging protected works, control information, and administrative information; and

- The VDE "Control" – a mechanism for defining the regimen for using protected information that is inside a secure container.

3. Professor Maier will describe the background of a person of ordinary skill in the art. Such a person would understand the claims in light of the required capabilities and architectural features above.

4. The specification set forth in the '193 patent has numerous inconsistencies in its terminology. Some inconsistencies concern the data hierarchy (e.g., methods, control information, component assemblies). Other examples include the description of a non-secure host event processing environment and the concept of containment.

The following further summarizes Professor Maier's opinions.

I. EXPLANATION OF U.S. PATENT NO. 6,253,193

A. Asserted Capabilities of the Virtual Distribution Environment

The '193 Patent describes a system that is asserted to be the first universal, distributed processing system for persistently controlling digital information. This system was given the name "Virtual Distribution Environment" or "VDE". As described in the Patent, VDE promised at least the following mandatory features:

1. the creation of a comprehensive data security and commerce world;

2. the ability to handle all types of digital works independent of computing platform, making it a single, general purpose solution in contrast to multiple, limited solutions;

3. flexible control mechanisms that can be applied to any granularity of content;

4. control mechanisms that are configurable by any user, not just the system designers or content providers; and

5. isolation of the system programs and protected works from the non-VDE world, preventing observation, interference, or removal from the VDE, except as permitted by the VDE control mechanisms.

Although these features are promised by the '193 Patent, this does not mean that they are necessarily achievable.

1. Comprehensive Data Security and Commerce World

According to the '193 Patent, VDE is described as being the only comprehensive solution in a world of limited solutions. VDE is described as an end-to-end solution for digital works that guarantees the authenticity, confidentiality and integrity of the works and the VDE mechanisms. These protections are promised to be effective against any unauthorized activity by a third party (i.e. a user other than the creator of the work) that has physical possession of the computing hardware and wishes to circumvent the protections.

VDE must provide the ability to control the distribution and usage of digital works as well as tracking, reporting, auditing and handling payment for the distribution and usage. Additionally, VDE must support multiple business models simultaneously, for example, time-based and volume-based charging for the same digital work or licensing digital works with or without added sub-licensing rights.

Only those systems that are members of the electronic commerce world can participate in VDE commerce transactions. Consequently, all transactions must occur between

member systems since there is no way to control digital works that are outside the boundaries of the VDE world.

2. General Purpose

According to the '193 Patent, the VDE system is the only rights management solution needed by its users because it is capable of handling and protecting all types of digital works, such as digital audio, digital video, software, digital cash, digital documents, electronic publications, etc. within a single rights management framework, whereas previous systems handled only limited subsets of information types. It further states that VDE can function within all types of electronic devices, from smart cards, pagers and telephones to supercomputers.

3. Flexible

According to the '193 Patent, the VDE system can manage protected works in arbitrarily sized data chunks, down to the smallest atomic element. The Patent distinguished prior art systems that used access controls that were limited to the file level or resource level. The VDE system is described as being able to meter, track, bill and audit the usage of these arbitrary data chunks in addition to controlling the access to those data chunks. For example, a consumer can be charged by the number of bytes downloaded or by the number of paragraphs printed. Additionally, each of these actions can be specified independently, such that two objects can be metered differently, but billed identically.

This flexibility allows two different users to be charged at different rates, for different granularities, and in different currencies for using the same digital work. The '193 Patent distinguished prior art systems that lacked this flexibility.

4. Controls Configurable by All Users

According to the '193 Patent, the VDE system protects a digital work from the instant it is placed under VDE control subject to the permissions provided by the object creator (or rights holder) at the same or at another VDE "secure node." (The nature of the "secure node" is discussed later.) From that moment, the digital work becomes encapsulated within a VDE container. Then, the creator must grant permissions for accessing and distributing the digital work within the VDE object as well as identify how the object can be handled by other users of the VDE world.

These other users can create additional VDE-based controls for this protected work. In general, these controls only impose additional restrictions on the VDE object because they cannot conflict with the creator's VDE controls (except in the limited case in which the creator allows his controls to be modified by other users.) Even the end user is permitted to add VDE controls to VDE objects that he has received.

VDE controls are said to be persistent in that become permanently associated with the protected work once they are received, and they cannot be removed or deleted except as permitted by so-called "senior" VDE controls.

5. System Isolation

According to the '193 Patent, VDE protected works can only be accessed using VDE-certified foundation hardware and software. As a fundamental requirement, the VDE

foundation must isolate the internal workings of the system from the user because the user is not trusted.

Each computing device in the VDE world constitutes a "secure node" that must provide a "protected processing environment" (PPE) composed of VDE-certified foundation hardware and software. Sensitive materials such as protected works, administrative information, control information, and VDE software components, are passed between the protected processing environments of secure nodes inside "secure containers" that shield the materials from outside observation and alteration while in transit or in storage. The PPE must also shield all processing of the materials inside the PPE and also prevent the materials or process state information from "leaving" the VDE except as authorized by VDE control information. If the system fails to keep a protected work secret, then it can be distributed freely from that point onward. If the system fails to prevent alteration, then the consumer may receive invalid information (e.g., a bad stock quote), the consumer may receive less value than that for which he bargained (e.g., digital cash token that has been devalued), or the consumer's computer may be damaged by malicious code (e.g., virus-infected software), just to name a few examples. If the system fails to prevent the materials or process state information from leaving, then it can be moved to a system outside the VDE control regime for examination, manipulation, replication, or analysis.

Electronic devices outside the VDE world do not incorporate the VDE foundation, and hence are not constrained by VDE protocols. Thus, protected works are not permitted to be in clear text form outside of the isolated and rigidly controlled protected processing environment.

To guarantee the isolation and integrity of the PPE, the VDE foundation software itself must be protected by storing it in a location that is inaccessible to the user or by encrypting it when it is stored at a location that can be observed by the user.

B. VDE Core Architecture

According to the '193 Patent, three constituent building blocks are necessary to implement the VDE world:

1. VDE Foundation Hardware and Software – installed throughout an infrastructure of interlinked computing devices, each of which is called a "secure node";
2. The VDE "Secure Container" – a mechanism for packaging protected works, control information, and administrative information; and
3. The VDE "Control" – a mechanism for defining the regimen for using protected information that is inside a secure container.

Both controls and protected works are transferred between secure nodes by means of the secure container mechanism. Secure containers can be opened (and the protected works used) only within the protected processing environment of a secure node by executing VDE controls that regulate and track such activity.

The proper combination of these three building blocks isolates internal processing from the untrusted user (by creating an unbypassable foundation of hardware and software); isolates protected works from the untrusted user (by placing them in a shielded data structure); and provides a control mechanism that will allow the untrusted user to make use of the protected works only under controlled conditions.

1. VDE Foundation Hardware/Software

The VDE foundation hardware and software must ensure that the competing interests of both the owner and user of protected works are respected. The owner has an interest in controlling the distribution of his digital works and in compelling the reporting and payment for such use. The user has an interest in the control of his computing device, his privacy, and the availability of digital works for which he has paid.

The VDE foundation hardware and software must provide a sequestered venue in which external authority dominates the user's local authority in the control of information and processing. This VDE foundation hardware and software is the basis for any VDE installation on a device

A VDE secure node is a device that provides a VDE installation incorporating VDE foundation hardware and software as the base stratum on which all VDE functions are executed. In any secure node where protected works are used or where VDE control information is created or modified, a VDE secure subsystem core must be present. This core is enclosed by a "tamper resistant security barrier" that prevents observation of, interference with, and leaving of information and processes except as authorized by VDE control information.

This VDE secure subsystem core handles encrypting and decrypting data and code, storing control and metering information, managing secure communication with other VDE secure subsystem cores at other secure nodes, dynamically assembling and executing VDE control procedures, and updating control information for protected works.

Control procedures for the promised permission checking, metering, billing, and budget management features all execute within the VDE secure subsystem core.

The VDE foundation hardware and software must guarantee that control procedures triggered by user or system events are executed correctly and completely in the VDE secure subsystem core. Both correctness and completeness are necessary to preserve the integrity of VDE control regime. Failure can compromise the rights, privacy, or financial interests of the owner or user of the protected works.

According to the '193 Patent, these functions are provided and enforced by a secure processing unit (SPU) that is protected by a special purpose physical enclosure (the tamper resistant security barrier) that conceals the underlying VDE processing from observation or interference by external persons or processes, and that destroys information rather than allow the information to leave the VDE subsystem core via unauthorized means.

The '193 Patent suggests that a tamper resistant security barrier might be simulated solely in software by using several known software techniques, but it gives no specific direction as to how these techniques can be applied to achieve the guarantees required by the VDE secure subsystem core in an environment that is under the control of an untrusted user.

2. VDE Secure Containers

An invariant requirement of the VDE container concept is that no access or use can be made of the protected works within a VDE container except as regulated by associated VDE control information. This associated control information can be provided in the

same secure container that holds the protected works or it can be provided independently in a separate secure container.

In addition to the protected works included within a secure container, there can be references to other digital works stored external to the container. However, the container cannot regulate other access or usage to these externally stored digital works. ("Containment" is discussed further is Section IV. D.)

VDE secure containers can contain administrative information, such as auditing, tracking, and billing requests and reports.

The internal structure of a VDE secure container must be able to store independently manageable digital works. Subsections of a VDE secure container can be encrypted by different keys, including subdivisions of a single digital work.

The internal structure of a VDE secure container must be able to store other VDE secure containers nested inside it. Each nested container is subject to its own independent control information. Control information corresponding to the outer container may not override more restrictive control information that corresponds to a secure container nested within it.

The VDE secure container supports modification of its contents and its control information subject to the current corresponding control information.

Because of this capability, a VDE secure container may be empty in the sense that it does not contain a digital work while it does contain control information that identifies the digital work that can be added to the secure container. Thus, a VDE secure container can be used as a mobile agent to retrieve digital works from remote locations.

3. VDE Controls

According to the '193 Patent, the configurability and flexibility of the VDE system arises jointly from the modular and independently selectable nature of control information and the dynamic construction and execution of control procedures within the VDE secure subsystem of a computing device. As used herein, the VDE secure subsystem refers to the VDE foundation hardware and software residing within the tamper resistant security barrier.

VDE controls are executable procedures constructed by the VDE foundation as a response to a request to access or use a specific protected work. The control is constructed inside the VDE secure subsystem using VDE control information. VDE control information is composed of executable code, rule information that is enforced by the executable code, and blueprint instructions for constructing the executable control. The VDE secure subsystem guarantees that the control procedure is constructed according to the blueprint instructions and that the components used in the construction are authentic as to source, identity, and data integrity.

All use of protected works is regulated by corresponding control information that is used to construct each executable control procedure. Different control procedures can regulate auditing, billing, metering, tracking and usage events (such as printing, rendering, copying, etc.) with respect to individual users for a single instance of a protected work. These events cannot occur except as regulated by the execution of the individual control procedures. Additionally, these control procedures can be applied at arbitrarily fine levels of granularity, such as charging for the number of bytes read.

Any VDE user can define control procedures to the extent permitted by senior VDE control information.

Control information is deliverable independent of the protected work. Individual portions of control information are deliverable independent of each other. Control information made by added, modified, or replaced over time to the extent permitted by earlier control information. Because independent control information for any given instance of a protected work can be created by different sources at different locations and different times, the control information from these sources can be in conflict. VDE must supply a means for resolving these conflicts. According to the '193 Patent, the executable controls negotiate to determine the conditions under which a protected work may be used. Thus, controls are said to "evolve" over time.

Once delivered to a VDE node with the corresponding protected work, control information persists throughout the life of the protected work.

The VDE controls must support a broad range of control regimes, all of which can co-exist on a single VDE secure node.

Dynamic assembly and execution of a VDE control must occur within the VDE secure subsystem. Construction of a VDE control from its component parts in a non-VDE system allows unconstrained access to digital works. Thus, VDE control information is transmitted between secure nodes using VDE secure containers and stored at VDE nodes in encrypted form whenever outside the VDE secure subsystem.

Executable control procedures are constructed from load modules, data, and VDE methods. These control procedures are assembled and executed in response to user and

system events. According to some statements in the '193 Patent, a "component assembly" is a VDE control procedure.

C. Claim Interpretation

A person of ordinary skill in the art would understand the claims of the '193 Patent in light of the mandatory capabilities and architectural components described above.

D. Summary of Internal Inconsistencies.

The '193 Patent contains numerous internal inconsistencies. Examples of these inconsistencies are given below.

1. Use of Quotations

Hundreds of terms are set off in quotations throughout the specification. These terms include: detail description, virtual distribution environment, electronic highway, VDE aware, content, virtual, things, chain of handling and control, rules and controls, CD ROM, information utility, switch, transaction processor, usage analyst, operating system, method, budget, atomic, firmware, hash bucket, peripheral device, event-based, multi-threaded, locking, Remote Procedure Call, two-phase commit, and read only. Some of these terms are coined (such as VDE aware; rules and controls; and usage analyst) while many are well known computer concepts (such as operating system and Remote Procedure Call.).

In many cases, it is unclear whether any particular use of quotation marks was intended to introduce a coined term, to indicate figurative or metaphorical usage of a term, to indicate non-standard or a weakened usage of a term, or something else

2. System Availability

In the Absract, the '193 Patent asserts that "the invention . . . maintain[s] the integrity, availability, and/or confidentiality" of protected works. However, the system described does not appear to be designed to guarantee the availability of protected works. Rather, any deviation from the expected processing sequence is considered to be evidence of an attempt to crack the system or steal the protected works. In response, the system is likely to halt all processing until a trusted VDE administrator intervenes and resets the system. Additionally, the '193 Patent uses denial of service to enforce reporting obligations imposed by a rights holder. This practice is not consistent with preserving availability of digital works.

3. "Container" vs. "Object"

There is no consistent delineation in the '193 Patent between the terms "container" and "object." Initially, there appears to be a distinction in that the container is a shell data structure that is encapsulating data and the object is the combination of the container data structure and the encapsulated data. See Fig. 5A. Elsewhere, this distinction is blurred by the use of such phrases as:

"secure object (content container)";

"VDE content container is an object"; and

"VDE container (object)",

which appear to make container and object synonymous.

4. The Property of Being "Contained"

In the '193 Patent, there is no clear definition for the term "contain." The '193 patent states at one point that a container such as "container 302 may 'contain' items without those items actually being stored in the container." This definition of "contain" to include "referencing" is not customary in information storage terminology.

Subsequent examples in the '193 indicate that "contain" and "reference" are distinct relationships. For example, "may contain or reference" is used numerous times such as in "Load modules 1100 may contain or reference other load modules." and as in "Container 300y may contain and/or reference. . . ."

5. Inconsistent Data Structure Hierarchy

The hierarchy and relationships amongst rules, controls, methods, load modules, control information, and other data structures is inconsistent.

a) "Rules and Controls" vs. "Control Information"

The term "control information" is defined in the "Background and Summary of the Invention" of the '193 Patent as: ". . . load modules, associated data and methods . . ."

Later, the specification uses the phrase " 'rules and controls' (control information)" as if the phrases "control information" and "rules and controls" are synonymous. Further, it states that "rules and controls" can be in the form of: "a 'permissions record' 808; 'budgets' 308 and 'other methods' 1000", but makes no mention of load modules.

Subsequent uses of "control information" such as: ". . . other aspects of the information to be contained within the object (e.g., rules and control information, identifying

information, etc.)"; and "the user may specify permissions, rules and/or control information." indicate that rules are different and distinct from control information.

b) "Component Assembly" vs. "Control Information"

In the '193 Patent, the relationship between component assembly and control information in the data hierarchy is defined inconsistently. Contrast the statement:

> "In this example control information may include one or more component assemblies that describe the articles within such a container (e.g. one or more event methods referencing map tables and/or algorithms that describe the extent of each article)."

with:

> ". . . control information (*typically a collection of methods related to one another by one or more permissions records, including any method defining variables*) . . ." [italics in original]
>
> "This "channel 0" "open channel" task may then issue a series of requests to secure database manager 566 to obtain the "blueprint" for constructing one or more component assemblies 690 to be associated with channel 594 (block 1127). In the preferred embodiment, this "blueprint" may comprise a PERC 808 and/or URT 464.'

In one case, the component assembly is a part of control information, but in the other case, control information is separable from and describes how to build a component assemblies.

c) **"Budgets"**

According to the '193 Patent, "budgets" are a special type of "method". Methods are defined as containing, among other things, "User Data Elements". Elsewhere, budgets are cited as a common type of User Data Element. This inconsistency creates confusion as to whether any given use of the term "budget" refers to an executable method or a non-executable data structure.

6. **"Load Module"**

According to the '193 Patent, executable code is provided in the form of "'atomic' load modules", presumably meaning that they are the smallest unit of executable code. Later, however, load modules are sub-dividable into smaller load modules, which is inconsistent with atomicity.

7. **The "Non-Secure" "Protected Processing Environment"**

According to the '193 Patent, a necessary feature of a VDE computer is the "protected processing environment" or "PPE". Secure Event Processing Environments ("SPE"), in which all sensitive processing is handled inside a hardware device called a Secure Processing Unit ("SPU") are stated as being one type of PPE. Host Event Processing Environments ("HPE") are also said to be a type of PPE. The HPE classification is further described as having two sub-types: secure and non-secure. Additionally, the specification defines the three abbreviations as synonymous and interchangeable starting at column 103 of the specification, unless the context of any given passage indicates otherwise.

Further, no criteria are provided for distinguishing between a "secure HPE" and a "non-secure HPE". Thus, it is not possible to reconcile the "non-secure HPE" as a secure operating environment or protected processing environment.

EXHIBIT H

Mini Markman 30 Terms/Phrases to Address

1. Set forth below are the twelve claims designated for the "Mini-Markman" proceeding.
2. The parties, in accordance with the Court's February 21, 2003, Order, have agreed to narrow the "Mini-Markman" proceeding to a selected thirty terms and phrases, set forth in boldface below.
3. Bold denotes the terms and the phrases that the parties have designated to be construed in the "Mini-Markman" proceeding; underscoring denotes the designation is a phrase.
4. Bolding of the claim number indicates that Microsoft construes the claim as a whole as requiring its "Global Construction" of "VDE."

U.S. Patent No. 6,253,193

1. A method comprising:
receiving a digital file including music;
storing said digital file in a first **secure** memory of a first device;
storing information associated with said digital file in a **secure** database stored on said first device, said information including at least one **budget control** and at least one **copy control**, said at least one **budget control** including <u>**a budget specifying the number of copies which can be made of said digital file**</u>; and said at least one <u>**copy control controlling the copies made of said digital file**</u>;
determining whether said digital file may be **copied** and stored on a second device based on at least said **copy control**;
if said **copy control** allows at least a portion of said digital file to be **copied** and stored on a second device,
copying at least a portion of said digital file;
transferring at least a portion of said digital file to a second device including a memory and an audio and/or video output;
storing said digital file in said memory of said second device; and
including playing said music through said audio output.

11. A method comprising:
receiving a digital file;
storing said digital file in a first **secure** memory of a first device;
storing information associated with said digital file in a **secure** database stored on said first device, said information including a first **control**;
determining whether said digital file may be **copied** and stored on a second device based on said first **control**,
said determining step including identifying said second device and determining whether said first **control** allows transfer of said **copied** file to said second device,

said determination based at least in part on the features present at the device to which said **copied** file is to be transferred;

if said first **control** allows at least a portion of said digital file to be **copied** and stored on a second device,

copying at least a portion of said digital file;

transferring at least a portion of said digital file to a second device including a memory and an audio and/or video output;

storing said digital file in said memory of said second device; and

rendering said digital file through said output.

15. A method comprising:

receiving a digital file;

an **authentication** step comprising:

accessing at least one **identifier** associated with a first device or with a user of said first device; and

determining whether said **identifier** is associated with a device and/or user authorized to store said digital file;

storing said digital file in a first **secure** memory of said first device, but only if said device and/or user is so authorized, but not proceeding with said storing if said device and/or user is not authorized;

storing information associated with said digital file in a **secure** database stored on said first device, said information including at least one **control**;

determining whether said digital file may be **copied** and stored on a second device based on said at least one **control**;

if said at least one **control** allows at least a portion of said digital file to be **copied** and stored on a second device,

copying at least a portion of said digital file;

transferring at least a portion of said digital file to a second device including a memory and an audio and/or video output;

storing said digital file in said memory of said second device; and

rendering said digital file through said output.

19. A method comprising:

receiving a digital file at a first device;

establishing communication between said first device and a **clearinghouse** located at a location remote from said first device;

said first device obtaining authorization information including a key from said **clearinghouse**;

said first device using said authorization information to gain access to or make at least one **use** of said first digital file, including using said key to decrypt at least a portion of said first digital file; and

receiving a first **control** from said **clearinghouse** at said first device;

storing said first digital file in a memory of said first device;

using said first **control** to determine whether said first digital file may be **copied** and stored on a second device;

if said first **control** allows at least a portion of said first digital file to be **copied** and stored on a second device,

copying at least a portion of said first digital file;

transferring at least a portion of said first digital file to a second device including a memory and an audio and/or video output;

storing said first digital file portion in said memory of said second device; and

rendering said first digital file portion through said output.

U.S. Patent No. 6,185,683

2. A system including:

a first apparatus including,

user **controls,**

a communications port,

a processor,

a memory storing:

a first **secure container containing** a governed item, the first **secure container** governed item being at least in part encrypted; the first **secure container** having been received from a second apparatus;

a first **secure container** rule at least in part governing an **aspect** of access to or **use** of said first **secure container** governed item, the first **secure container** rule, the first **secure container** rule having been received from a third apparatus different from said second apparatus; and

hardware or software used for receiving and opening **secure containers**, said **secure containers** each including the capacity to **contain** a governed item, a **secure container** rule being associated with each of said **secure containers**;

a **protected processing environment** at least in part protecting information **contained** in said **protected processing environment** from tampering by a user of said first apparatus, said **protected processing environment** including hardware or software used for applying said first **secure container** rule and a second **secure container** rule in combination to at least in part govern at least one **aspect** of access to or **use** of a governed item **contained** in a **secure container**; and

hardware or software used for transmission of **secure containers** to other apparatuses or for the receipt of **secure containers** from other apparatuses.

U.S. Patent No. 6,157,721

1. A security method comprising:

(a) **digitally signing** a first load module with a first **digital signature designating** the first load module for **use** by a first **device class;**

(b) **<u>digitally signing a second load module with a second digital signature different from the first digital signature, the second digital signature designating the second load module for use by a second device class having at least one of tamper resistance and security level different from the at least one of tamper resistance and security level of the first device class</u>**;

(c) distributing the first load module for **use** by at least one device in the first **device class**; and

(d) distributing the second load module for **use** by at least one device in the second **device class**.

34. A **protected processing environment** comprising:

a first **tamper resistant barrier** having a first security level,

a first **secure** execution space, and

at least one arrangement within the first **tamper resistant barrier** that prevents the first **secure** execution space from executing the same **executable** accessed by a second **secure** execution space having a second **tamper resistant barrier** with a second security level different from the first security level.

U.S. Patent No. 5,920,861

58. A method of creating a first **secure container**, said method including the following steps;

accessing a descriptive data structure, said descriptive data structure including or addressing

organization information at least in part describing a required or desired organization of a content section of said first **secure container**, and

metadata information at least in part specifying at least one step required or desired in creation of said first **secure container**;

using said descriptive data structure to organize said first **secure container** contents;

using said metadata information to at least in part determine specific information required to be included in said first **secure container** contents; and

generating or identifying at least one rule designed to **control** at least one **aspect** of access to or **use** of at least a portion of said first **secure container** contents.

U.S. Patent No. 5,982,891

1. A method for using at least one resource processed in a **secure** operating environment at a first appliance, said method comprising:

securely receiving a first entity's **control** at said first appliance, said first entity being located remotely from said operating environment and said first appliance;

securely receiving a second entity's **control** at said first appliance, said second entity being located remotely from said operating environment and said first appliance, said second entity being different from said first entity; and

securely processing a data item at said first appliance, using at least one resource, including **<u>securely applying, at said first appliance through use of said at least one resource said first entity's control and said second entity's control to govern use of said data item</u>**.

U.S. Patent No. 5,892,900

155. A **virtual distribution environment** comprising
a first **host processing environment** comprising
a central processing unit;
main memory operatively connected to said central processing unit;
mass storage operatively connected to said central processing unit and said main memory;
said mass storage storing tamper resistant software designed to be loaded into said main memory and executed by said central processing unit, said tamper resistant software comprising:
machine check programming which **derives information from one or more aspects of said host processing environment**,
one or more storage locations storing said information;
integrity programming which causes said machine check programming to **derive** said information, **compares** said information to information previously stored in said one or more storage locations, and
generates an indication based on the result of said **comparison**; and
programming which takes one or more actions based on the state of said indication;
said one or more actions including at least temporarily halting further processing.

U.S. Patent No. 5,917,912

8. A process comprising the following steps:
accessing a first record **containing** information directly or indirectly identifying one or more elements of a first **component assembly**,
at least one of said elements including at least some **executable programming**,
at least one of said elements constituting a load module,
said load module including **executable programming** and a header;
said header including an execution space **identifier** **identifying at least one aspect of an execution space required for use and/or execution of the load module** associated with said header;
said execution space **identifier** provides the capability for distinguishing between execution spaces providing a higher level of security and execution spaces providing a lower level of security;
using said information to identify and locate said one or more elements;
accessing said located one or more elements;
securely assembling said one or more elements to form at least a portion of said first **component assembly**;
executing at least some of said **executable programming**; and
checking said record for validity prior to performing said executing step.

35. A process comprising the following steps:
at a first processing environment receiving a first record from a second processing environment remote from said first processing environment;

said first record being received in a **secure container**;

said first record **containing** identification information directly or indirectly identifying one or more elements of a first **component assembly**;

at least one of said elements including at least some **executable programming**;

said **component assembly** allowing access to or **use** of specified information;

said **secure container** also including a first of said elements;

accessing said first record;

using said identification information to identify and locate said one or more elements;

said locating step including locating a second of said elements at a third processing environment located remotely from said first processing environment and said second processing environment;

accessing said located one or more elements;

said element accessing step including retrieving said second element from said third processing environment;

securely assembling said one or more elements to form at least a portion of said first **component assembly** specified by said first record; and

executing at least some of said **executable programming**,

said executing step taking place at said first processing environment.

EXHIBIT I

PLR 4-3(a) – Constructions on Which the Parties Agree

	Claim Term / Phrase	Agreed Construction
1.	**entity** 891.1	Any person or organization.
2.	**generating** 861.58	Producing.
3.	**govern, governed, governing** 891.1, 683.2	See Control (v.).
4.	**metadata information** 861.58	Information that describes one or more attributes of other data, and/or the processes used to create and/or use that data. For example, metadata information may describe the following attributes of other data: its meaning, representation in storage, what it is used for and by whom, context, quality and condition, location, ownership, or its data elements or their attributes (name, size, data type, etc.)
5.	**rendering** 193.11, 193.15, 193.19	In the context of 193.11, 15 and 19: Playing content through an audio output (e.g., speakers) or displaying content on a video output (e.g., a screen).
6.	**secure container rule** 683.2	A "rule" that governs (Controls) a Secure Container "governed item."
7.	**security** 721.1, 721.34	See Secure.
8.	**tampering** 683.2, 721.1, 721.34, 900.155	Using (e.g., observing or altering) in any unauthorized manner, or interfering with authorized use.
9.	**"said mass storage storing tamper resistant software"** 900.155	The "tamper resistant software" is physically stored within, as opposed to being merely "addressed" by, the mass storage.
10.	**"including using said key to decrypt at least a portion of said first digital file"** 193.19	The "at least one use of said digital file" must encompass decrypting at least a "portion" of the "digital file" using the "key."

KEKER & VAN NEST, LLP
JOHN W. KEKER - #49092
MICHAEL H. PAGE - #154913
710 Sansome Street
San Francisco, CA 94111-1704
Telephone: (415) 391-5400
Facsimile: (415) 397-7188

DERWIN & SIEGEL, LLP
DOUGLAS K. DERWIN - #111407
3280 Alpine Road
Portola Valley, CA 94028
Telephone: (408) 855-8700
Facsimile: (408) 529-8799

INTERTRUST TECHNOLOGIES CORPORATION
JEFF MCDOW - #184727
4800 Patrick Henry Drive
Santa Clara, CA 95054
Telephone: (408) 855-0100
Facsimile: (408) 855-0144

Attorneys for Plaintiff and Counter-Defendant
INTERTRUST TECHNOLOGIES CORPORATION

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

INTERTRUST TECHNOLOGIES CORPORATION, a Delaware corporation, Plaintiff, v. MICROSOFT CORPORATION, a Washington corporation, Defendant.	Case No. C 01-1640 SBA (MEJ) Consolidated with C 02-0647 SBA **MEMORANDUM OF POINTS AND AUTHORITIES OF PLAINTIFF INTERTRUST TECHNOLOGIES IN OPPOSITION TO MICROSOFT MOTION FOR SUMMARY JUDGMENT ON INDEFINITENESS AND IN SUPPORT OF CROSS-MOTION FOR SUMMARY JUDGMENT**
AND COUNTER ACTION.	Date: May 30, 2003

TABLE OF CONTENTS

TABLE OF CONTENTS
(cont'd)

TABLE OF AUTHORITIES

Page(s)

Cases

TABLE OF AUTHORITIES
(cont'd)

Statutes

I. INTRODUCTION

The word "secure" is widely used in the computer security field. It appears in the claims of hundreds of patents, including many issued to Microsoft. It is used in product documentation, technical literature and white papers published by Microsoft and others. It is defined in numerous technical dictionaries, including the Microsoft Computer Dictionary.

Yet Microsoft now seeks to convince the Court that the word "secure," when used in InterTrust patent claims, is so vague that it renders those claims indefinite as a matter of law.

InterTrust's patents are presumed valid, and Microsoft carries a heavy burden of establishing, by clear and convincing evidence, that one of ordinary skill in the art would be unable to understand or apply the claims. This burden is considerably heavier where, as here, the disputed term is widely used by the defendant, by others in the field, and in numerous patents.

Microsoft cannot possibly carry its burden. It relies on a test manufactured by its expert witness, Professor Mitchell, for the purpose of this litigation, a test never applied to any other document, a test that is so stringent that it is failed by Microsoft patents, third party patents and industry documents. In fact, Professor Mitchell's published papers fail his own test! There is no evidence that any document ever created anywhere, by anyone, can pass Prof. Mitchell's test.

InterTrust's patents use the term "secure" in a manner consistent with the generally understood use of that term in the industry. Microsoft uses the term in exactly the same manner in its own patents and documents. Microsoft cannot carry its burden. InterTrust therefore seeks summary judgment that the disputed claims are definite.

II. FACTS

A. "Secure" and "Security" Are Widely Used in the Computer Security Field.

The terms "secure" and "security" are widely used in the computer security field to refer to the application of one or more mechanisms to protect a computer system or process against attack. Mitchell Decl., 4:18-19; Reiter SJ Decl., ¶¶ 5-7.[1]

[1] Declaration of Dr. Michael Reiter in Opposition to Microsoft Motion for Summary Judgment on Invalidity and In Support of InterTrust's Cross-Motion.

1. **General use in the industry.**

a. Dictionary definitions. "Secure" and "security" are defined in many computer dictionaries. Those definitions use different language, but consistently focus on protection against a type of attack or misuse. Reiter SJ Decl., ¶ 7(a); McDow Decl., ¶ 5 and Ex. C.[2]

b. Microsoft and third party documentation. Microsoft routinely uses the words "secure" and "security" to refer to its own products. Reiter SJ Decl., ¶¶ 14-22, 27. For example, Microsoft describes how its Windows operating system was evaluated under a standard security methodology, including statements such as "Windows 2000 meets the evaluation requirements by providing secure directory access and administration." This document also describes features such as "secure connectivity," "secure policy application," and "secure networked environment." Reiter SJ Decl., ¶ 16 and Ex. J. This use of "secure" to describe products or product features is common in Microsoft documents. Reiter SJ Decl., ¶ 27 and Ex. C, Page Decl., Ex. C.

Dr. Reiter analyzed publicly-available Microsoft technical documents that use the term "secure." They do not pass Prof. Mitchell's test. Reiter SJ Decl., ¶ 27 and Ex. C.

Microsoft's use of "secure" to refer to its products and features is not limited to public documents. In internal documents, Microsoft engineers describe products as "secure," with no apparent difficulty in understanding what the term means. These include terms that are identical or extremely similar to the terms Prof. Mitchell has decided are "unclear." Derwin Decl.,¶¶ 3-6.[3]

"Secure" is also routinely used in third party documents without definition. Reiter SJ Decl., ¶7(b) and Ex. L, Page Decl., Ex. B.

2. **Use in Prof. Mitchell's papers.**

Prof. Mitchell's papers use the term "secure" or "securely." Dr. Reiter applied Prof. Mitchell's test to these papers. The papers do not pass the test. Reiter SJ Decl., ¶ 26 and Ex. F.

---

[2] Declaration of Jeff McDow in Opposition to Microsoft Motion for Summary Judgment on Invalidity and In Support of InterTrust's Cross-Motion.

[3] Declaration of Douglas Derwin In Opposition to Microsoft Motion for Summary Judgment and In Support of InterTrust's Cross-Motion.

3. Use in other patents.

a. Microsoft patents. The term "secure" is used as an adjective or adverb describing computer products or processes in the claims of numerous Microsoft patents, including one of the patents Microsoft has asserted against InterTrust in a counterclaim in this action. McDow Decl., ¶ 6 and Ex. D; Reiter SJ Decl., ¶¶ 7(c), 28 and Ex. D.

Microsoft's patents include claims with terms such as: "secure mode," "securely stores," "secure function," "securely shared," "secure access," "secure network," "secure data," "securely integrated," "secure message" and "secure package." McDow Decl., Ex. D.

Dr. Reiter analyzed a number of the Microsoft patents. None of them passes Prof. Mitchell's test. Indeed, the Microsoft patents contain less information about what "secure" means than do the InterTrust patents. Reiter SJ Decl., ¶ 29.

b. Third party patents. Ex. E to the McDow Decl. illustrates the use of "secure" in the claims of 100 computer-related patents issued over the past year, including phrases such as "secure element," "secure server," secure environment" "secure Internet access," "secure storage device," secure data" and "secure operating system." Dr. Reiter checked several of these patents, none of which can pass Prof. Mitchell's test. None of them includes as much information about what "secure" means as do the InterTrust patents. Reiter SJ Decl., ¶¶ 30-31.

B. Recognized Methodologies Exist for Determining if Computer Products or Methods are Secure.

Dr. Reiter describes several recognized methodologies for determining if computer products are "secure," some of which are explicitly referenced in the InterTrust patents. Reiter SJ Decl., ¶¶ 13-23. Computer security professionals routinely use such methodologies to determine if products or methods are "secure," and purchasers (including the U.S. Government) routinely rely on these determinations in making purchasing decisions. Reiter SJ Decl., ¶ 13.

Dr. Reiter's Declaration includes a description of a Microsoft marketing document explaining how one such methodology was applied to Microsoft Windows, and declaring that elements of the product had been found to be "secure." Reiter SJ Decl., ¶¶ 14-22 and Ex. J.

The information included in the InterTrust patents includes guidance regarding how

security should be measured, including the statement that security should be based on a commercially reasonable standard.[4] Computer security professionals routinely apply such a standard in building security into real-world products. Reiter SJ Decl., ¶¶ 12, 18.

C. The Experts Agree on the General Meaning of "Secure" and "Security."

InterTrust and Microsoft have each proposed a definition for "secure." Those definitions are generally consistent, the primary difference being Microsoft's insistence that each of five specific properties be protected, whereas InterTrust's definition is: "One or more mechanisms are employed to prevent, detect, or discourage misuse of or interference with information or processes." This definition is definite, it is easily understood and simply applied, and provides clear guideposts for determining whether a specific system falls within its scope.

Microsoft's expert, Professor Mitchell and InterTrust's expert, Dr. Reiter, agree that "secure" and "security" have a general meaning in the field. Reiter SJ Decl., ¶ 5. In his Declaration, Prof. Mitchell explains this general meaning:

> In computer science, including the particular fields most pertinent to these InterTrust patents, "security" generally has to do with designs, techniques and mechanisms for protecting certain properties against some kinds of attack or adversarial conditions.

Declaration of Professor John C. Mitchell ("Mitchell Decl."), 4:15-17. Prof. Mitchell's deposition testimony, quoted at McDow Decl., Ex. A, § 1, is consistent with this understanding:

> A. Well, security generally has to do with guaranteeing certain properties against some kind of attack or adversarial conditions.

Mitchell I, 29:6-8.[5]

> We use the word "secure" to suggest that there are some properties being protected against an adversarial attack.

Mitchell I, 88:5-7.

> I mean, ordinarily, and almost uniformly, "security" is a term that suggests one or more properties against one or more threats where the properties and threats are determined by the context in which you use it.

---

[4] See, e.g., items 19(B) and 19(J) from Joint Claim Construction Statement, Ex. C, which contains InterTrust's evidence in support of its claim construction position.

[5] In transcript quotations, extraneous material (e.g., objections) is omitted.

Mitchell I, 117:8-12.

Professor Mitchell also testified that those of ordinary skill in the art can determine if a product is "secure" through commonly used methodologies or criteria. That testimony, which is quoted in McDow Decl., Ex. A, § 2, includes the following:

Q. Is it ever possible to determine if a system is secure, in your opinion?

A. There are compelling arguments that can be presented to substantiate a claim of security. There's a recognized set of criteria, or several proposed sets of criteria, for establishing or certifying security systems.

Mitchell I, 46:20-47:1.

Q. So I take it that there are a range of methods that a security analyst might use to determine if a system is secure, correct?

THE WITNESS: Yes. A security analyst, given a set of properties and a set of possible attacks or looking for attacks, could use a number of different methods to study a system.

Q. Was that also true as of February 1995?

A. I believe so.

Mitchell I, 53:11-21.

Prof. Mitchell's testimony on this issue is clear, consistent and unambiguous:

(a) "Secure" means that properties of a system are protected against attacks.

(b) To determine if a particular system is "secure," it is necessary to perform an investigation to determine what the protected properties are, what the potential attacks are, and whether the former are protected against the latter.

(c) There are recognized methodologies used to perform this investigation.

D. The InterTrust Patents Use the Terms "Secure" and "Security" Consistently with the Generally Accepted Meaning of these Terms.

Prof. Mitchell understands what "secure" means in the patents. His testimony is quoted at McDow Decl., Ex. A, § 3. Following are some of the highlights:

A. I don't find any place in the patent where it says, "In this document, 'secure' means the following." So in that sense, I don't really see a definition of "security" here.

However, the patent describes or suggests or promises a set of properties, and

they include these five properties, as I understand it.

Q. Okay. And these five properties are the properties availability, secrecy, integrity, authenticity, and nonrepudiation that are listed in the Microsoft construction for "secure," correct?

A. I believe that's what we're discussing, yes.

Mitchell I 68:25-69:11.

Were you able in some cases to determine what the patent meant by the use of the word "secure"?

A. I'm having a little trouble putting my finger on or imagining a specific case to give you as an example. But there are some passages where there are descriptions of -- that are a little more specific and give some reasonable guess as to which of these properties are relevant in that situation.

Q. Are there some passages in the '193 patent in which the word "secure" is used to refer to a subset of these five properties?

THE WITNESS: Yeah. I mean, it may be in the sense I just described.

Mitchell I, 74:20-75:10.

Microsoft's argument that "secure" is used inconsistently in the InterTrust patents is based on a mischaracterization of the patents. Thus, Microsoft points out that the InterTrust patents use a variety of adjectives to modify "secure, and argues that "the meaning of these different degrees of security is unclear." MS Memo. at 10:20. The passages cited by Microsoft, however, explicitly explain the differences between many of these terms. Thus, "truly secure" and "less secure" occur in the same sentence, with the former characterizing processing using a Secure Processing Unit whereas the latter characterizes processing using a Host Processing Environment. '193 Patent, 80:22-35. These terms are not used in isolation, but are explicitly explained and contrasted. Similarly, the '193 patent contains a passage contrasting "highly secure" encryption algorithms with "extremely secure" algorithms, and explicitly identifies each type of algorithm, including explaining circumstances under which each should be used. '193 Patent, 67:18-40. See also '193 Patent, 201:63-202:12. Again, these uses are not evidence that "secure" is meaningless, but instead include significant clarifying detail, detail that Microsoft and Prof. Mitchell ignore. Each of these passages uses the term "secure," and each of them serves as an example of the meaning of the term "secure" in the claims (e.g., both "highly

secure" and "extremely secure" algorithms are "secure.")

Prof. Mitchell understands what "secure" means in the InterTrust patents: in general it means protection of the five listed properties, but sometimes the word refers to protection of fewer than all five. This testimony is consistent with InterTrust's proposed definition of "secure" and with Dr. Reiter's testimony. Reiter SJ Decl., ¶¶ 5 and 7(d).

E. Prof. Mitchell's Declaration Establishes that the Disputed Terms Are Definite and Clear.

Prof. Mitchell understands the meaning of the disputed terms. The first claim term analyzed in his Declaration is "secure memory." He first explains what the term means:

> Thus, the "secure memory" must at least be able to store a file whose copying or moving is prevented, except as authorized.

Mitchell Decl., 20:10-18.

Prof. Mitchell thus understands that a "secure memory" must prevent unauthorized copying or moving of a file.

Prof. Mitchell next discusses use of "secure memory" in the art (Mitchell Decl., 20:20-25), then turns to descriptions of the term in the patent specification. He quotes over 30 lines of detailed description from a specification embodiment of "secure memory," including protection mechanisms and the actions prevented (e.g., information cannot be observed, interfered with or leave except under appropriate conditions).

InterTrust may not agree with Prof. Mitchell's construction of "secure memory" when that phrase is presented for construction. Nevertheless, the fact that Prof. Mitchell is able to articulate a clear definition of the term demonstrates that "secure" is not indefinite.

The next term analyzed by Prof. Mitchell is "secure container." Again, he analyzes the term, extrinsic evidence and the specification and concludes as follows:

> This method [861.58] appears to promise that it prevents anyone and anything from accessing or using certain information (by putting the information in a secure container), except as authorized by a rule. (Mitchell Decl., 26:3-6)

> The component assembly [in 912.35] is protected in at least three ways: (a) one of its elements is shielded from unauthorized access (by a secure container), (b) the record identifying the elements necessary to build the component assembly is

likewise protected . . . .(Id., 26:22-26)

This language from '683, Claim 2 . . . suggests that the 'secure container' is able to prevent 'an aspect of access to or use of' its governed items . . . .(Id., 27:22-25)

Thus, Prof. Mitchell understands "secure container" similarly in all three claims: the container shields or protects its contents from access or use.

Similar points can be made about Prof. Mitchell's discussion of the other purportedly indefinite claim terms: in each case his Declaration reveals he understands what the term means.

Prof. Mitchell's opinion that "secure" is indefinite is not based on any failure to understand the claim terms, but instead on InterTrust's failure to meet a ten-part test that takes up two pages in his Declaration. Mitchell Decl., 9:3-11:4. However, Prof. Mitchell admitted in his deposition that he had created this test for purposes of this litigation, after deciding that more standard methodologies were too "technical" for the Court to understand. Mitchell II, 223:13-16. McDow Decl., Ex. A, § 5, Reiter SJ Decl., ¶¶ 2, 24. Tellingly, Prof. Mitchell made no attempt to apply his test to any other document. See Mitchell testimony in McDow Decl., Ex. A, § 6.

Not surprisingly, when Prof. Mitchell's test is applied in other contexts, it turns out that Microsoft's security-related technical documentation also fails his test, Microsoft's patents fail his test, third party patents fail his test, and Prof. Mitchell's own computer security papers fail his test. Reiter SJ Decl., ¶¶ 25-32 and Exs. C-F.

Moreover, Prof. Mitchell's application of this test is revealing. For example, he does not feel that InterTrust's "secure memory" meets test item (2), since "There is no indication, e.g., of what information in addition to the file is to be stored." Mitchell Decl., 23:8-9.

The relevant claim (193.1) states that the secure memory contains a digital file. It does not require any other information, and Prof. Mitchell does not argue that the claim includes any such requirement. Mitchell II, 292:17-293:17. Thus, InterTrust fails his test because the claim does not identify other information the presence of which is not required by the claim.

Similarly, Prof. Mitchell testifies that item (3) from his test hasn't been met since "There is no clear indication of whether the stored information's availability, integrity or authenticity is

to be protected." Mitchell Decl., 23:10-11. Earlier in the Declaration, however, he noted that the claim requires that copying or moving the file be prevented, except as authorized. Mitchell Decl., 19:10-11. Similarly, he understands specification references to "secure memory" to mean that "a 'secure memory' is 'secure' in part because all unauthorized access to, observation of, and interference with information stored within it is prevented." Mitchell Decl., 21:11-14.

Thus, according to Prof. Mitchell, the claim and the specification embodiment clearly explain what is being protected.[6] Prof. Mitchell does not explain why it is necessary for the claim to also list other elements the protection of which is not required by the claim.

To take one last example, Prof. Mitchell finds "secure operating environment" indefinite despite the following: "The patents suggest that a 'secure operating environment' is 'secure' in part because it prevents all unauthorized access to, and observation of, and interference with data and processes within the operating environment." Mitchell Decl., 33:7-9. Despite this, Prof. Mitchell nevertheless finds the term indefinite because it doesn't pass his test.

Prof. Mitchell understands the claim terms, but argues they are unclear because they do not include enough information to pass his made-up ten-part test, including information that is clearly extraneous to the claim. The Federal Circuit has a name for analysis of this type: semantic quibbling. Rosemount, Inc. v. Beckman Instruments, Inc., 727 F.2d 1540, 1548 (Fed. Cir. 1984).[7] Microsoft cites no legal support for the proposition that a claim may be invalidated for indefiniteness based on its failure to recite extraneous details. No such support exists.

F. The InterTrust Patents Contain Significant Information About Every Element of Prof. Mitchell's Test.

Even if Prof. Mitchell's test were accepted in the industry, InterTrust's patents contain a

---

[6] InterTrust does not necessarily agree with Prof. Mitchell's interpretation of "secure memory" or other terms he discusses. Those terms may have to be construed by the Court in subsequent proceedings, and InterTrust will present its position on their meaning at that time. The significance of Prof. Mitchell's testimony is not that he agrees with InterTrust's interpretation of the claims, but that he has no difficulty coming to an interpretation, thereby clearly indicating that the claims are not indefinite. That parties disagree about the meaning of the claims does not render them indefinite. See below, § III B 3.

[7] "Beckman attacks the claims as indefinite, primarily because 'close proximity' is not specifically or precisely defined. . . . [T]o accept Beckman's contention would turn the construction of a patent into a mere semantic quibble that serves no useful purpose."

wealth of detail responsive to every element of that test, detail that Prof. Mitchell ignores. Reiter SJ Decl., ¶ 38 and Ex. B, § II. Prof. Mitchell's ignorance of key passages is understandable, since InterTrust identified specification passages of greatest significance to the disputed terms, but Microsoft failed to provide this information to him. McDow Decl.,¶¶ 9-10 and Ex. A, § 8. These passages provide significant detail on the terms, including very important elements not described in the passages quoted in Prof. Mitchell's Declaration. Reiter SJ Decl., ¶¶ 44-48.

III. ARGUMENT

A. Microsoft Carries a Heavy Burden of Establishing Indefiniteness By Clear and Convincing Evidence.

InterTrust's patents carry a "strong presumption of validity," and the burden is on Microsoft to rebut that presumption with "clear and convincing evidence." Al-Site Corp. v. VSI Int'l, Inc., 174 F.3d 1308, 1323 (Fed. Cir. 1999); Intel Corp. v. Via Techs., Inc., 319 F.3d 1357, 1366 (Fed. Cir. 2003) ("Any fact critical to a holding on indefiniteness, moreover, must be proven by the challenger by clear and convincing evidence"). In ruling on Microsoft's indefiniteness defense, the Court must resolve close questions in favor of InterTrust. Exxon Research & Eng'g Co. v. United States, 265 F.3d 1371, 1380 (Fed. Cir. 2001).

B. Indefiniteness Standards.

In Exxon Research, the Federal Circuit provided an overview of the indefiniteness analysis, emphasizing the difficult burden facing a party seeking to establish that the claims of an issued U.S. Patent are invalid for indefiniteness:

> In determining whether that standard is met, i.e., whether "the claims at issue [are] sufficiently precise to permit a potential competitor to determine whether or not he is infringing," we have not held that a claim is indefinite merely because it poses a difficult issue of claim construction. We engage in claim construction every day, and cases frequently present close questions of claim construction on which expert witnesses, trial courts, and even the judges of this court may disagree. Under a broad concept of indefiniteness, all but the clearest claim construction issues could be regarded as giving rise to invalidating indefiniteness in the claims at issue. But we have not adopted that approach to the law of indefiniteness. We have not insisted that claims be plain on their face in order to avoid condemnation for indefiniteness; rather, what we have asked is that the claims be amenable to construction, however difficult that task may be. If a claim is insolubly ambiguous, and no narrowing construction can properly be adopted, we have held the claim indefinite. If the meaning of the claim is discernible, even

> though the task may be formidable and the conclusion may be one over which reasonable persons will disagree, we have held the claim sufficiently clear to avoid invalidity on indefiniteness grounds. By finding claims indefinite only if reasonable efforts at claim construction prove futile, we accord respect to the statutory presumption of patent validity and we protect the inventive contribution of patentees, even when the drafting of their patents has been less than ideal.

Exxon Research, 265 F.3d at 1375 (citations omitted).

1. Whether one of ordinary skill in the art would understand the claim.

To carry its burden, Microsoft must establish that one of ordinary skill in the art would not be able to understand the scope of the claims, read in light of the specification. North Am. Vaccine v. American Cyanamid Co., 7 F.3d 1571, 1579 (Fed. Cir. 1993). In making this determination, the Court must keep in mind that patents are not required to include information that would be understood by one of ordinary skill:

> Patent documents are written for persons familiar with the relevant field; the patentee is not required to include in the specification information readily understood by practitioners, lest every patent be required to be written as a comprehensive tutorial and treatise for the generalist, instead of a concise statement for persons in the field. Thus resolution of any ambiguity arising from the claims and specification may be aided by extrinsic evidence of usage and meaning of a term in the context of the invention. The question is not whether the word "substantially" has a fixed meaning as applied to "constant wall thickness," but how the phrase would be understood by persons experienced in this field of mechanics, upon reading the patent documents.

Verve, LLC v. Crane Cams, Inc., 311 F.3d 1116, 1119-20 (Fed. Cir. 2002).

2. Use of general terms to describe a range of circumstances does not render claims indefinite.

Claims may use general terms to describe a range of circumstances, as long as those of ordinary skill in the art would be able to understand the terms. In Exxon Research, the Federal Circuit found a claim term not indefinite despite the fact that the presence of the claim element would depend on external factors, including the conditions chosen for the claimed process:

> Although the patent does not quantify the "period sufficient" limitation by reference to any specific period or range of periods, it does not leave those skilled in the art entirely without guidance as to the scope of that requirement. . . .
>
> * * *
>
> Because the patent makes clear that the period in question will vary with changes in the catalyst and the conditions in which the process is run, we conclude that the claim limitation is expressed in terms that are reasonably precise in light of the

subject matter.

Exxon Research , 265 F.3d at 1379.

Similarly, in Orthokinetics, Inc. v. Safety Travel Chairs, Inc., 806 F.2d 1565, 1576 (Fed. Cir. 1986), the Federal Circuit held that a claim term was not indefinite despite the use of general language the application of which would necessarily depend on the circumstances:

> [Claim] 1. In a wheel chair having a seat portion, a front leg portion, and a rear wheel assembly, the improvement wherein said front leg portion is so dimensioned as to be insertable through the space between the doorframe of an automobile and one of the seats thereof . . . .
>
> * * *
>
> The claims were intended to cover the use of the invention with various types of automobiles. That a particular chair on which the claims read may fit within some automobiles and not others is of no moment. The phrase "so dimensioned" is as accurate as the subject matter permits, automobiles being of various sizes. As long as those of ordinary skill in the art realized that the dimensions could be easily obtained, § 112, 2d para. requires nothing more. The patent law does not require that all possible lengths corresponding to the spaces in hundreds of different automobiles be listed in the patent, let alone that they be listed in the claims.

Orthokinetics, 806 F.2d at 1576 (citation omitted).

Thus, in Orthokinetics the Federal Circuit held "so dimensioned" to be sufficiently definite, despite the fact that a chair "so dimensioned" as to fit into one car would not necessarily fit into another car. The Federal Circuit held that it was unnecessary for the patentee to list all of the possible dimensions in the claim, or in the body of the patent itself. This ruling is in direct contrast to Microsoft's methodology.

The district courts have held similarly, rejecting indefiniteness arguments based on claim elements the presence of which depends on external circumstances:

> As with selectivity, whether an antibody has a useful degree of affinity appears to depend on several factors. Genentech's expert, Dr. Unkeless, testified at his deposition that the affinity value required for an antibody to work for purposes of diagnosis may vary depending on the type of assay that is used.
>
> * * *
>
> . . . If, as Dr. Unkeless suggests, it is impossible to define a useful level of affinity by reference to a particular numerical value, the '561 patent cannot be expected - and is not required as a matter of law - to list every possible affinity value that might be useful for every possible purpose of the invention.

> Moreover, simply because a broad range of affinities may be useful does not make the claims indefinite. It is well settled that breadth is not to be equated with indefiniteness." . . . Thus, the claims may permissibly encompass a wide range of affinity values . . . . The relevant question is whether a person of ordinary skill in the art would understand when a monoclonal antibody has an affinity value that is "useful" for the purposes described in the specification.

Chiron Corp. v. Genentech, Inc., No. Civ. S-00-1252, 2002 U.S. Dist. LEXIS 19150, *10-11 (E.D. Cal. June 24, 2002) (citations omitted).[8]

> The Court . . . finds that the term "substantial" as used in the context of paving installations described in the '550 Reissue Patent is sufficiently precise to inform one skilled in the art. . . . in the context of paving installations like those described in the '550 Reissue Patent which can be subjected to a wide variety of loads, it is understood that no explicit quantification can be made for such forces. Thus, the term "substantial" cannot be interpreted to mean a specific quantity; rather it describes a range of loads from pedestrian to vehicular to occasional heavy truck. Dr. Witczak further testified that while tractor-trailers and commercial aircraft would certainly produce "substantial" forces, it is understood from the patent that this invention would not be applied in installation subject to such forces. . . .
>
> * * *
>
> The Court finds that the term "substantial," when considered in the light of the entire claimed invention, is as accurate as the subject matter permits and provides sufficient guidance to one skilled in the art of paving stone installations. . . . Given that pedestrians and vehicles come in a myriad of shapes and sizes, it would be impossible to set forth every possible specific force. Thus, the use of the term "substantial forces" adequately explains that walkways and driveways which incorporate this interlocking paving installation can be subjected to a limited range of forces - from pedestrians up to heavy trucks.

Pave Tech, Inc. v. Snap Edge Corp., 952 F. Supp. 1284, 1301-02 (N.D. Ill. 1996) (citations omitted).

Thus, the case law is clear that patent claims may use general, and even relative, language, where that language is understood by those in the art, and a patentee is not required to provide a comprehensive description of all circumstances in which infringement may be found, but can instead use general language where a comprehensive description would be impractical.

Microsoft's motion is premised on the theory that "secure" is indefinite because determining whether a particular system is "secure" requires an evaluation of the context. MS Memo. at 2:6-18.. As Exxon Research, Orthokinetics, Chiron and Pave Tech make clear, a claim

[8] A copy of this opinion is attached as Ex. R to the Page Decl.

is not rendered indefinite because its application depends on context, nor because it uses general terms that may apply differently in different circumstances.

3. That reasonable persons might disagree regarding the scope of the claims does not render the claims indefinite.

The fact that reasonable people may disagree regarding the application of a claim term does not render that term indefinite:

> It may of course occur that persons experienced in a technologic field will have divergent opinions as to the meaning of a term, particularly as narrow distinctions are drawn by the parties or warranted by the technology. Patent disputes often raise close questions requiring refinement of technical definitions in light of particular facts. The judge will then be obliged to decide between contending positions; a role familiar to judges. But the fact that the parties disagree about claim scope does not of itself render the claim invalid.

Verve, LLC v. Crane Cams, Inc., 311 F.3d 1116, 1120 (Fed. Cir. 2002). See also Exxon Research, 265 F.3d at 1375 (claims not indefinite even if "expert witnesses, trial courts, and even the judges of this court may disagree"). Thus, the fact that InterTrust and Microsoft have proffered similar, but distinct definitions does not suggest that the claims are indefinite.

4. Claims are not indefinite merely because work is required to determine the scope of the claims, as long as such work is not beyond the abilities of one of ordinary skill.

Patent claims are not indefinite merely because determining their scope requires "trial and error" or experimentation, as long as "undue" experimentation is not required:

> The district court invalidated both patents for indefiniteness because of its view that some "trial and error" would be needed to determine the "lower limits" of stretch rate above 10% per second at various temperatures above 35 degrees C. That was error. Assuming some experimentation were needed, a patent is not invalid because of a need for experimentation. . . . A patent is invalid only when those skilled in the art are required to engage in *undue* experimentation to practice the invention. In re Angstadt, 537 F.2d 498, 503-04, 190 U.S.P.Q. 214, 218 (C.C.P.A. 1976). There was no evidence and the court made no finding that undue experimentation was required.

W.L. Gore & Associates, Inc. v. Garlock, Inc., 721 F.2d 1540, 1557 (Fed. Cir. 1983). The test for "undue experimentation" is whether this would require "ingenuity beyond that to be expected of one of ordinary skill in the art." In re Angstadt, 537 F.2d 498, 503-04 (C.C.P.A. 1976).[9]

---

[9] This case involved enablement, rather than definiteness, but has been cited by the Federal Circuit (e.g., W.L. Gore, cited above) as describing the undue experimentation test applied to indefiniteness.

C. Microsoft's Two-Part Test for Finding Indefiniteness Has Been Rejected By the Federal Circuit.

Microsoft argues that indefiniteness is determined using a two-part test, including whether the claim is "as precise as the subject matter permits" (MS Memo. at 21:9-10) and argues that InterTrust's use of "secure" was not as precise as possible. Memo. at 12:25-13:23.

Microsoft misstates the law. The Federal Circuit has repeatedly held that § 112(2) does not require that claims be drafted as precisely or specifically as possible:

> Claims are often drafted using terminology that is not as precise or specific as it might be. As long as the result complies with the statutory requirement to "particularly point[] out and distinctly claim[] the subject matter which the applicant regards as his invention," 35 U.S.C. § 112, para. 2, that practice is permissible.

PPG Indus., Inc. v. Guardian Indus. Corp., 156 F.3d 1351, 1355 (Fed. Cir. 1998).

> The trial court was correct to fault the Exxon patents as lacking in specificity in several respects--specificity that in some instances would have been easy to provide and would have largely obviated the need to address the issue of indefiniteness. As is often the case when problems in document drafting lead to litigation, the ideal of precision was not achieved here, and we are left to deal with an imperfect product. While we agree with the trial court that the product was less than perfect, we disagree that the flaws were fatal.
>
> * * *
>
> . . . The patentee could easily have cured the ambiguity by adding a single word or phrase to the claims or specification . . . . In fact, much of the extrinsic evidence suggests that the practice in this field of art is to state specifically whether velocity is interstitial or superficial. That practice was not followed in the '982 patent, and the result is that there is some question as to the proper interpretation of the claims. The question we must answer is whether the claims are rendered so ambiguous that one of skill in the art could not reasonably understand their scope. . . .
>
> * * *
>
> If this case were before an examiner, the examiner might well be justified in demanding that the applicant more clearly define UL, and thereby remove any degree of ambiguity. However, we are faced with an issued patent that enjoys a presumption of validity. In these circumstances, we conclude that a person of skill in the art would understand the scope of the term U[L], and that the degree of ambiguity injected into the claims by the patentee's lack of precision is therefore not fatal.

Exxon Research, 265 F.3d at 1376, 1383-84.

Microsoft's argument was discussed in an opinion summarizing Federal Circuit law and concluding that the Federal Circuit does not require that patent claims be drafted as precisely as

the subject matter permits:

> Citing Amgen, Alcon takes the position that a claim must be as precise as the subject matter permits. The court in Amgen did state that "claims must ... be 'as precise as the subject matter permits.'" 927 F.2d at 1217. That statement, however, was contained in a parenthetical characterization of the holding in Shatterproof Glass Corp. v. Libbey-Owens Ford Co., 758 F.2d 613 (Fed. Cir.), cert. denied, 474 U.S. 976, 88 L. Ed. 2d 326, 106 S. Ct. 340 (1985)), but the court in Shatterproof Glass did not actually state that claims must be as precise as the subject matter permits. Rather, the court there stated that "if the claims, read in the light of the specifications, reasonably apprise those skilled in the art both of the utilization and scope of the invention, and if the language is as precise as the subject matter permits, the courts can demand no more.'" Id. at 624 (quoting Georgia-Pacific Corp. v. United States Plywood Corp., 258 F.2d 124, 136 (2d Cir.), cert. denied, 358 U.S. 884, 3 L. Ed. 2d 112, 79 S. Ct. 124 (1958)) (emphasis added).
>
> Were these the only two cases on the issue, there might be some ambiguity as to whether being as precise as the subject matter permits is a necessary, or merely a sufficient, condition for a claim to pass muster under § 112. Federal Circuit cases do not insist on the kind of precision urged by Alcon. The Federal Circuit has never said that all claims must be made as precise as humanly possible, without exception. In fact, in a case decided after Amgen, the court observed that "claims are often drafted using terminology that is not as precise or specific as it might be. As long as the result complies with the statutory requirement to 'particularly point[ ] out and distinctly claim[ ] the subject matter which the applicant regards as his invention,' 35 U.S.C. § 112, para. 2, that practice is permissible." PPG Indus. v. Guardian Indus. Corp., 156 F.3d 1351, 1355 (Fed. Cir. 1998).
>
> The focus, then, is whether, given the nature of the subject matter, the claim is precise enough to make clear to a person skilled in the art what is claimed. There may be times when, for one reason or another, it is impossible, unnecessary, or undesirable to state a claim in terms of precise, quantified measurements. See, e.g., United States v. Telectronics, Inc., 857 F.2d 778, 786 (Fed. Cir. 1988) (district court erred as a matter of law in holding that if claim were read to mean that electric current must be applied "so as to minimize fibrous tissue formation," it would be invalid under § 112 because it would be "impossible to determine when sufficient minimization takes place to determine what current range is involved"), cert. denied, 490 U.S. 1046, 104 L. Ed. 2d 423, 109 S. Ct. 1954 (1989). That is permissible as long as the dictates of § 112 are met.

Bausch & Lomb, Inc. v. Alcon Labs., Inc., 79 F. Supp. 2d 243, 245 (W.D.N.Y. 1999).

Microsoft misstates Federal Circuit law in precisely the same way as the defendant in Bausch & Lomb. Microsoft's two-part indefiniteness test is wrong.

D. The Undisputed Facts Establish that "Secure" and "Security" Are Definite.

1. Use of the term in the industry.

"Secure" and "security" are widely used in the computer security field. Reiter SJ Decl., ¶¶ 5-7. Acceptance of a term by the industry is evidence that use of the term does not render

patent claims indefinite. Rosemount, Inc. v. Beckman Instruments, Inc., 727 F.2d 1540, 1547 (Fed. Cir. 1984); Advanced Cardiovascular Sys., Inc. v. Scimed Life Sys., 96 F. Supp. 2d 1006, 1019 (N.D. Cal. 2000).

2. Use of the term by the defendant in describing its own products.

Microsoft routinely describes its products and features as "secure," both in public documents and in internal documentation. See above, § II A 1(b). The defendant's use of the disputed term supports finding that term not indefinite. Rosemount, 727 F.2d at 1547; Advanced Cardiovascular Systems, 96 F. Supp. 2d at 1019.

3. Use of the term in other patents, including the defendant's patents.

As is described in § II A 3 above, Microsoft's patents use "secure" and "securely" in a manner similar to the InterTrust claims, and these terms are routinely used in claims of third party patents (at least 100 in the past year alone). This supports finding the term to be definite:

> The criticized words are ubiquitous in patent claims. Such usages, when serving reasonably to describe the claimed subject matter to those of skill in the field of the invention, and to distinguish the claimed subject matter from the prior art, have been accepted in patent examination and upheld by the courts.

Andrew Corp. v. Gabriel Electronics, Inc., 847 F.2d 819, 821 (Fed. Cir. 1988).

> Genentech's use of similar terminology without apparent difficulty . . . in its own patent applications, is yet another indication that what is meant by a "useful degree of affinity" is not indefinite. . . .
>
> . . . Genentech's use of the phrase "sufficient affinity" in its own patent application belies its contention that one of ordinary skill in the art would not understand when an antibody has sufficient affinity to be "useful" for therapy.

Chiron Corp., 2002 U.S. Dist. LEXIS 19150, *14-16.[10]

> Indeed, one of Alcon's own witnesses . . . though stating that he did not know what the term "does not substantially inhibit" means in the '607 patent, admitted on cross-examination that several of Allergan's own patents, including some on which Anger himself was named as an inventor, use similar language.
>
> *   *   *
>
> There was also evidence that Alcon itself has used the word "substantially" in its own patents and in proceedings before the Patent and Trademark Office ("PTO").

Bausch & Lomb, Inc. v. Alcon Labs., Inc., 79 F. Supp. 2d 243, 250 (W.D.N.Y. 1999).

---

[10] Page Decl., Ex. R.

4. Ability of the Examiner to apply the terms to the prior art.

The PTO Examiners assigned to the InterTrust applications had no difficulty applying the disputed terms (including secure, secure container and protected processing environment) to the prior art. McDow Decl., ¶ 8 and Ex. G. For example, in the Sept. 22, 1998 Notice of Allowance for InterTrust's'019 patent, the Examiner stated that "there is no disclosure [in the prior art Fischer patent] of the recited three secure containers as set forth in the instant claims." He had no difficulty understanding the term "secure containers" or determining whether a "secure container" was disclosed in the prior art. This is one of numerous Patent Office documents quoted in McDow Decl., Ex. G in which Examiners of different InterTrust patents used the term "secure" or a variant and showed that they understood its meaning and were able to apply it.

This supports finding the claims definite. SDS USA, Inc. v. Ken Specialties, Inc., 107 F. Supp. 2d 574, 596 (D.N.J. 2000) (Examiner determining that claim element was found in prior art reference, patent held not indefinite: "SDS accurately surmises from that comment that the 'transfer unit' was readily recognizable to Examiner Crane, and presumably to other skilled professionals, based on mechanisms found in the prior art.").

E. Prof. Mitchell's Analysis Should Be Disregarded, Since He Admittedly Made No Attempt to Understand the Meaning of "Secure" in the Context of the Claims as a Whole.

Prof. Mitchell improperly analyzed the term "secure" in isolation and not in the context of the entire claim in which the term appears. For example, as is described in § II E above, one factor leading Prof. Mitchell to conclude that "secure memory" is indefinite is the fact that the claim does not identify what information other than the digital file is contained in the secure memory, despite the fact that the claim does not require any other information. Prof. Mitchell's explanation revealed that his entire methodology is fatally flawed:

> Q. So, again, sir, is it your testimony that the secure memory recited in '193, claim 1 includes some information other than the digital file?
>
> A. Well, I don't think I have an opinion about it. That sounds like a question about the meaning of the claim, apart from the meaning of the phrase "secure memory."
>
> And, to this point, I haven't really been asked to form a clear

> understanding of the claim and haven't really reflected and done proper study on exactly the question you ask.

Mitchell II 297:2-12.

Thus, Prof. Mitchell believes that "secure memory" is "unclear" in claim 193.1 because (among other things) although the claim indicates a "digital file" is stored in the memory it doesn't identify other information stored in the memory. When asked whether the claim requires such other information, however, he testified that he hadn't studied the claim itself and had no opinion. This testimony was not a momentary aberration:

> Q. Well, does '193, claim 1, require that anything other than the digital file be stored in the secure memory recited in that claim?
>
> THE WITNESS: That sounds like a question about the meaning of the claim rather than a meaning of the phrase "secure memory" to me.
>
> Q. Okay. Does that mean you can't answer the question?
>
> A. To the -- I believe so.

Mitchell II, 298:3-23.

Thus, Prof. Mitchell has no opinion regarding the manner in which "secure memory" is used in the claim, and admits that he doesn't know whether his analysis (e.g., other stored information must be identified) is relevant to the claim, since he hasn't analyzed the claim.

The analysis of indefiniteness begins with the claims themselves:

> Only after a thorough attempt to understand the meaning of a claim has failed to resolve material ambiguities can one conclude that the claim is invalid for indefiniteness. Foremost among the tools of claim construction is of course the claim language itself, but other portions of the intrinsic evidence are clearly relevant, including the patent specification and prosecution history.

All Dental Prodx, LLC v. Advantage Dental Prods., Inc., 309 F.3d 774, 780 (Fed. Cir. 2002).

Prof. Mitchell was not asked to and did not analyze the meaning of the claims and therefore, for example, had no opinion regarding whether one of the elements he felt should be defined as part of "secure memory" was in fact required by the relevant claim. His testimony on indefiniteness was not based on an interpretation of the phrase in the context of the claim. He therefore failed to apply the proper legal standard and his testimony should be disregarded.

F. Microsoft's Evidence, Analogies and Case Support Are Either Irrelevant or Inaccurate.

1. Depositions of third parties.

Microsoft relies heavily on third party testimony regarding the meaning of disputed terms. As is discussed more fully in InterTrust's Motion to Strike, served and filed herewith, these witnesses are not qualified as of ordinary skill in the art, nor have they read the patents, and their testimony is therefore incompetent and should be stricken. If the Court admits this testimony, InterTrust has also included other testimony that establishes that the witnesses understand the disputed terms and can apply them, as well as an explanation of Microsoft's mischaracterization of that testimony. McDow Ex. B, §§ 1(b), 2(b),(c),(d), 3(b),(c).

2. Microsoft's Car and Safe Analogies Are Irrelevant.

Microsoft attempts to convince the Court that "secure" is indefinite because there is no way to know what would be meant if someone characterized a car or a safe as "secure." MS Memo. at 3:13-27; Mitchell Decl., 57-13. These analogies are irrelevant, since the fact that the word "secure" might have no meaning in one context (e.g., a "secure rock") is irrelevant to whether it has meaning in another context in which it is routinely used (e.g., computer security).

3. Microsoft's Argument Relies on Cases that are either Irrelevant or Miscited.

The case discussed at greatest length in Microsoft's brief is Ex Parte Brummer, 12 U.S.P.Q.2d (BNA) 1653 (B.P.A.I. 1989), which Microsoft characterizes as "comparable" to the present case. MS Memo. at 22:13-15. Brummer involved an appeal from a Patent Office decision rejecting patent claims. 12 U.S.P.Q.2d at 1653. The Federal Circuit has warned that the indefiniteness analysis applied to issued patents (e.g., the InterTrust patents) is different than and requires a higher standard than the analysis applied to patent applications (e.g., Brummer). This is the result of the presumption of validity provided to issued patents, a presumption that does not apply to unissued patent applications. Exxon Research , 265 F.3d at 1380. See also, Solomon v. Kimberly-Clark Corp., 216 F.3d 1372, 1378-79 (Fed. Cir. 2000) (different standards applicable to indefiniteness analysis during patent examination and during litigation on issued patent means that evidence properly considered to establish indefiniteness during examination

should not be considered to establish indefiniteness in litigation).[11]

The difference between the indefiniteness standard applied to patent applications and the standard as applied to issued patents is illustrated by the differing outcomes in Brummer and Orthokinetics, cases each involving patent claims drafted in the context of the environment in which the patented item would be used. In Orthokinetics, claims were found definite despite the fact that those claims included an element described as dimensioned so as to fit into an automobile. The Federal Circuit noted that different dimensions would be required for different automobiles, but upheld validity of the claims nevertheless. Orthokinetics, 806 F.2d at 1576.

Microsoft also discusses In re Lechene, 277 F.2d 173 (C.C.P.A. 1960), at some length, arguing that an element discussed in that case ("stiff") is similar to "secure." MS Memo. at 22:6-12. Not only does this case involve an unissued patent application, the decision has nothing to do with definiteness under § 112(2). Instead, the opinion holds that claims were properly rejected as obvious based on a prior art reference. The opinion happens to use the word "indefinite," but in a context having nothing to do with § 112(2).

Microsoft relies on a 1938 case (General Electric Co. v. Wabash Appliance Corp., 304 U.S. 364 (1938)) for the proposition that "claim indefiniteness is particularly problematic where it derives from 'conveniently functional language at the exact point of novelty.'" MS Memo. at 23:7-8. That holding is irrelevant, however, since it involved a principle of claim construction (apparatus claims cannot include functional limitations) that was expressly overruled by the adoption of 35 U.S.C. § 112(6), and since Microsoft makes no argument that InterTrust's claims are indefinite based on inclusion of "functional" language.

Microsoft tries to shoehorn this into an indefiniteness argument by citing Dr. Reiter's testimony for the proposition that "security" is an "essential aspect" of the invention, and arguing that Exxon Research (cited above) stands for the proposition that it is "fatal for limitations critical to patentability to be indefinite." MS Memo. at 23:13-14.

This argument is wrong. First, Microsoft's characterization of Dr. Reiter's testimony is

---

[11] Microsoft's reliance on In re Cohn, 438 F.23d 989 (C.C.P.A 1971) (MS Memo. at 21:23-25) is misplaced for the same reason, since Cohn also involved an unissued patent application..

completely inaccurate. Reiter SJ Decl., ¶¶ 52-53. Second, Exxon Research contains no such holding. Instead, in Exxon Research the Federal Circuit distinguished an earlier decision on a number of grounds, one of which was the fact that the patent specification in the earlier case had characterized a limitation as critical to patentability, a factor not present in the Exxon Research case. The Federal Circuit noted that the Court of Customs and Patent Appeals had held that it was "not fatal for an applicant to express noncritical limitations with regard to factors such as time or quantity in functional rather than numerical terms." Exxon Research, 265 F.3d at 1379, citing In re Caldwell, 319 F.2d 254, 258 (C.C.P.A. 1963). The Federal Circuit neither stated nor implied that a different indefiniteness standard applies to "critical" limitations.

G. "Protected Processing Environment" and "Host Processing Environment" Are Not Indefinite

1. Protected Processing Environment.

Microsoft's discussion of Protected Processing Environment ("PPE") ignores extensive discussion in the specification. Thus, Microsoft complains that PPE is defined in terms of two other defined terms (HPE and SPE), and that defining one coined term with two other coined terms is "an unhelpful exercise." MS memo. at 18:11-13. Microsoft ignores, however, the specification's detailed description of SPEs and HPEs. Reiter SJ Decl., ¶¶ 39-40, Ex. G.

In addition, Microsoft passes lightly over the figures: "General reference is then made to the PPE in the 'Brief Description of the Drawings' but no meaningful discussion . . . ." MS Memo. at 17:25-26. This statement is false. Several of the drawings are explicitly described as relating to PPEs, and the patents contain dozens of pages describing these drawings. Reiter SJ Decl., ¶ 39-40 and Ex. G. Microsoft ignores all of this.

Prof. Mitchell finds "protected processing environment" indefinite based on his ten-part test. As with "secure," however, he has no difficulty understanding what the term means:

> The protected processing environment likewise shields the information it contains, again through the use of rules governing the access and use of the information. Information apparently cannot be used or accessed by anyone or anything without satisfaction of those associated, governing rules.

Mitchell Decl., 50:20-24.

Again, the issue is not whether InterTrust agrees with Prof. Mitchell's definition. For indefiniteness, the question is whether one of ordinary skill in the art can understand the term. Prof. Mitchell clearly has the ability to do so. His quibbles regarding the failure of the claims to specify every feature that is present (or absent) in a protected processing environment raise the same issues discussed above in connection with his application of his ten-part test to "secure."

2. Host Processing Environment.

Microsoft presents no evidence for its claim that "Host Processing Environment" is indefinite, except that the term was not in general use. Prof. Mitchell does not discuss this term.

Instead of evidence, Microsoft mischaracterizes the InterTrust patents, arguing that the term "host processing environment" is found in only a couple of locations in the patents, and that these locations do not clearly explain what the term means. MS Memo. at 19:7-24.

Microsoft's statement is highly misleading. Although the '900 patent discusses "host processing environments" in only a few locations, it contains extensive description of "HPEs." Reiter SJ Decl., ¶¶ 41-42. Microsoft was aware that the patent uses the acronym "HPE" to refer to Host Processing Environment (MS Memo. at 17:9), but chose to disregard the specification discussion of "HPEs" in favor of arguing that "host processing environments" were only discussed in a few places. This appears to be a deliberate attempt to mislead the Court.

H. The Foundational InterTrust Patent Application is Effectively Incorporated By Reference.

Microsoft seeks a ruling that would effectively invalidate three issued U.S. Patents as a result of a <u>clerical error</u> committed by the Patent Office. Those patents incorporate the original InterTrust application by reference, a procedure explicitly authorized by patent law. Microsoft's sole basis for complaint is that the application number was not later replaced by an issued U.S. patent number. Microsoft implies that this is improper because the original application was not available to those attempting to evaluate the later patents, but this is false, since the earlier application may be obtained from the Patent Office at minimal or no cost. No U.S. Patent has ever been invalidated based on the failure to replace an incorporated by reference application number with a patent number, and Microsoft carries a burden of establishing this issue by clear

and convincing evidence. InterTrust therefore seeks summary judgment on this issue.

According to Microsoft, the original InterTrust patent application is not properly incorporated by reference into three of the later-filed InterTrust patents. Microsoft characterizes the original application as "essential material" to these later patents. Microsoft Memo. at 12:7-9.

A patent that fails to incorporate "essential material" is invalid for lack of enablement. Quaker City Gear Works, Inc. v. Skil Corp., 747 F.2d 1446 (Fed. Cir. 1984). For this reason, Microsoft must establish the failure to incorporate by clear and convincing evidence. Intel Corp. v. Via Technologies, Inc. 319 F.3d 1357, 1366 (Fed. Cir. 2003).

The three InterTrust patents incorporate the earlier application by reference. McDow Decl., ¶ 11. Such incorporation is authorized by the MPEP. See MPEP § 608.01(p), reproduced in the Declaration of Karna J. Nisewaner ("Nisewaner Decl."), ¶ 4 and Ex. 1.

It has long been settled that a patentee's § 112 obligations may be met by materials incorporated by reference, as long as those materials are reasonably available to the public:

> We recognize that, subject to compliance with 35 USC 112 and 132, the disclosure in a patent application may be deliberately supplemented or completed by reference to . . . disclosure in earlier or concurrently filed copending applications, . . . or, in general, to "disclosure which is available to the public," . . . . As the expression itself implies, the purpose of "incorporation by reference" is to make one document become a part of another document by referring to the former in the latter in such a manner that it is apparent that the cited document is part of the referencing document as if it were fully set out therein.

In re Lund, 376 F.2d 982, 989 (C.C.P.A. 1967) (citations omitted).

> That total incorporation by reference cannot be accomplished under 112 is apparent from the reading of Lund, Heritage and Stauber. It is limited to reference to material available to the public. This would exclude secret or privileged materials as in the case of some abandoned patent applications. It is reasonable also to exclude materials which are not easily available to the public or the Patent Office. This would include unpublished dissertations and theses, obscure foreign publications and publications to which there are no available English translations.

General Electric Co. v. Brenner, 407 F.2d 1258, 1262-63 (D.C. Cir. 1968).

According to the MPEP, pending or abandoned applications are readily available. Nisewaner Decl., ¶ 4, Ex. 1. The InterTrust application may be obtained from the Patent Office. Nisewaner Decl., ¶¶ 6-9. In addition, the text of the application may be obtained for free in a

matter of minutes through the PTO's on-line service. Nisewaner Decl., ¶¶ 10-11. Microsoft's implication that incorporation of the original InterTrust application by reference was improper because that application is unavailable is false: the application is readily available to the public.

Microsoft argues that the reference to the incorporated InterTrust application should have been replaced with a reference to an issued patent. MS Memo. at 12:19-24. According to MPEP § 608.01(p), the examiner is supposed to replace an application number with the issued patent number. Microsoft cites no support for the argument that issued patents should be invalidated because of what amounts to a clerical mistake by the Patent Office, and it does not appear that any issued patent has ever been invalidated based on this theory. Microsoft cannot possibly carry its burden of showing invalidity by clear and convincing evidence, given the indisputable fact that the application is readily available at low cost. Summary judgment that the application was properly incorporated by reference, and the three patents are therefore not invalid for failure to include essential material is therefore proper.

Even if the foundational application had not been properly incorporated by reference, the later patents contain significant description of the allegedly indefinite terms, description that Microsoft simply ignores. Reiter SJ Decl.,¶ 43, Ex. H.

Microsoft has not carried its burden of establishing that these disclosures lack sufficient information for one of ordinary skill in the art to understand the claims of those patents in light of their specifications. Summary judgment should be entered against Microsoft on this issue.

IV. CONCLUSION

InterTrust respectfully requests that the Court deny Microsoft's motion for summary judgment and grant InterTrust's cross-motion for summary judgment.

Dated: April 7, 2003

DERWIN & SIEGEL, LLP

By: ______________________

DOUGLAS K. DERWIN
Attorneys for Plaintiff
INTERTRUST TECHNOLOGIES CORPORATION

WILLIAM L. ANTHONY (State Bar No. 106908)
ERIC L. WESENBERG (State Bar No. 139696)
HEIDI L. KEEFE (State Bar No. 178960)
ORRICK, HERRINGTON & SUTCLIFFE, LLP
1000 Marsh Road
Menlo Park, CA 94025
Telephone: (650) 614-7400
Facsimile: (650) 614-7401

STEVEN ALEXANDER (admitted *Pro Hac Vice*)
KRISTIN L. CLEVELAND (admitted *Pro Hac Vice*)
JAMES E. GERINGER (admitted *Pro Hac Vice*)
RICHARD D. MC LEOD (admitted *Pro Hac Vice*)
JOHN D. VANDENBERG
KLARQUIST SPARKMAN, LLP
One World Trade Center, Suite 1600
121 S.W. Salmon Street
Portland, OR 97204
Telephone: (503) 226-7391
Facsimile: (503) 228-9446

Attorneys for Defendant and Counterclaimant,
MICROSOFT CORPORATION

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

OAKLAND DIVISION

INTERTRUST TECHNOLOGIES CORPORATION, a Delaware corporation, Plaintiff, v. MICROSOFT CORPORATION, a Washington corporation, Defendant.	CASE NO. C01-1640 SBA (MEJ) **MICROSOFT'S MARKMAN BRIEF**
MICROSOFT CORPORATION, a Washington corporation, Counterclaimant, v. INTERTRUST TECHNOLOGIES CORPORATION, a Delaware corporation, Counter Claim-Defendant.	The Honorable Saundra B. Armstrong

TABLE OF CONTENTS

CASES

STATUTES/OTHER

I. INTRODUCTION

The claims must be read in light of the entire 900+ page "Big Book" patent application and, in particular, its 115 page "Summary of the Invention." This Summary of the Invention makes literally hundreds of statements touting the "important," "fundamental," "critical," and required features, capabilities and purposes of the "present invention." The Summary further defines this "invention" (which it expressly names "VDE") by distinguishing it from the allegedly "limited" and rigid solutions of others. All of these are required aspects of the "present invention," not merely optional features of a "preferred embodiment." As such, the claims must be read to include these "invention" features.

A. A Valid Claim Must Reflect This "Invention"

The Big Book's Summary of the Invention is InterTrust's elephant in the corner. The claim constructions urged by InterTrust are devoid of any of the required features of the "invention." InterTrust acts as if this "invention" simply did not exist. For example, the Big Book touts that VDE is able to prevent (not merely detect) all unauthorized access to protected content. Yet, InterTrust uniformly ignores this core promise of VDE security in its claim construction proposals, and instead urges that merely detecting misuse of content is sufficient.

InterTrust's whole approach is wrong. To ignore a patent's described "invention" when construing a patent claim, is contrary to patent law. "What is claimed by the patent application must be the same as what is disclosed in the specification; otherwise the patent should not issue." Festo Corp. v. Shoketsu Kinzoku Kogyo Kabushiki Co., 535 U.S. 722, 736 (2002). Thus, "it is fundamental that claims are to be construed in the light of the specifications and both are to be read with a view to ascertaining the invention." Adams v. United States, 383 U.S. 39, 49 (1966) (holding that patent claims required what the patent identified as an "object" of the "invention," even though the claims did not expressly recite that feature). Here, the Big Book's Summary of the Invention is critical to "ascertaining the invention."

B. These Twelve Claims Do Invoke This "Invention"

InterTrust's patent claims invoke the required features of the alleged "invention" in at least three ways.[1]

VDE Claim Terms: First, many of the key claim terms are VDE terms having special meanings in the VDE context. For example, the Big Book uses several general-sounding, functional terms (often a coined phrase) as short-hand labels for specific VDE mechanisms, such as "control," "container," "protected processing environment," and "virtual distribution environment." In these patents, a "control" is not whatever can exercise some kind (any kind) of control over something else; a "container" is not whatever can contain something; a "protected processing environment" is not any processing environment which is protected; and a "virtual distribution environment" is not any distribution environment which is virtual. Rather, these terms have special VDE meanings. For example, the Big Book defines its "virtual distribution environment" as a special breed: "The present invention provides a new kind of 'virtual distribution environment' (called 'VDE' in this document) that secures, administers, and audits electronic information use." ('193 2:24-27). These claim terms must be construed in their specific VDE sense, not some general sense divorced from the described "invention." (See Maier Decl. at 21-35.)

Vague Claim Terms: Second, most of the key claim terms are quite vague. These terms would deprive the claims of required clarity unless they are refined in light of the disclosed "invention." For example, ten of the mini-Markman claims use the terms "secure," "securely," and/or "protected." These claims do not specify how to distinguish a secure [something] from a non-secure [something], etc. Whether a "container" is "secure," for example, depends on the context, such as what is being protected, against what threats, for how long, and to what degree. (See Tran Decl. (Public) (assembling references); Keefe Decl. (assembling testimony: e.g., Shear Depo. at 100:19-101:23; Sibert Depo. at 97:20-25, 29:8-11); and the first Declaration of John

---

[1] Any claim that fails to invoke its specification's "invention" is invalid under 35 U.S.C. § 112, ¶ 1's "written description" requirement and ¶ 2's "regards as the invention" requirement. (See infra, Section V).

Mitchell (filed March 17, 2003).) As the claims do not expressly provide this required context, resort must be had to the disclosed "invention."[2] Many other claim terms also are sorely in need of definition from the specifications. (Cf. InterTrust Br. at 9:2-18).

VDE Claim Promises: Third, a core "invention" promise is the ability to prevent unauthorized access to (and use of) protected digital content notwithstanding myriad threats—identified in the Big Book—attempting to break or bypass that protection. (E.g., '193 221:19 et seq.) Each of the mini-Markman claims invokes this core VDE promise by promising to protect some content, process, and/or component. These promises of protection are unqualified. The claims identify no threat against which their promised protections are ineffective. The Big Book describes only one system for providing such "true" protection against these threats, and that is the complete VDE "invention." In other words, by requiring the promised protections supposedly afforded by the "invention," these claims invoke the required features of that "invention."

C. These Claims Demand Precise Constructions, True To The "Invention"

As InterTrust says, its proposed constructions are simple. They are simple, however, because (1) they are unfettered by the disclosed "invention" and its required capabilities and features touted in the Big Book's Summary of the Invention, (2) they treat the claims' specific VDE terms as general, non-VDE terms, (3) they ignore what each claim promises, and (4) they often are so vague as to be essentially meaningless.

InterTrust challenges Microsoft's constructions as complex. They are complex, because they honor precisely what the Big Book describes as the many required features of the "present invention." A proper construction of these claims necessarily is lengthy due to the sheer number of features the Big Book identifies as being "important" to its "invention." These required features are not "detailed limitations from specified embodiments," as charged by InterTrust (InterTrust Br. at 1:19-20), but rather the self-described "important" features of the "invention."

Simplicity and brevity are worthy goals in claim construction. But, they do not trump clarity and accuracy. Skilled persons faced with these claims would not dismiss any required

2 Here, InterTrust's specification is internally inconsistent and, in some ways, makes the scope of the claims even less clear. Consequently, Microsoft has moved for summary judgment of claim indefiniteness.

aspect of the Big Book's "invention." The sheer size of the Big Book should not frustrate the rules of claim construction, leave the public or jury guessing about a claim's precise boundaries, or divorce the claims from what the patent applicants touted as their "present invention."

II. SUMMARY OF ACCOMPANYING DECLARATIONS

The parties agree that this subject cannot be fully addressed in a 40-page brief. This Brief addresses some important features of the "invention" and some of the primary claim construction disputes. It is supplemented by the JCCS, and by the following declarations:

VDE's Features: The Declaration of Prof. David Maier, of Oregon Graduate Institute, describes the Big Book's "invention" and its mandatory features. To illustrate the operation of this "invention," he also explains the Big Book's only detailed example of how VDE handles a request to read protected content. Prof. Maier also describes some of the inconsistencies in the Big Book, including some that contradict passages cited by InterTrust.

"Security" And The Claims: Prof. John Mitchell, of Stanford, submitted a report on Microsoft's pending motion for summary judgment of claim indefiniteness. That report also pertains to claim construction. It explains how the label "secure" is "multi-dimensional, highly contextual, relative (i.e., a matter of degree), and subjective unless objectively defined." In his second Declaration, Prof. Mitchell explains how the "security" protections promised by the "invention" would have affected a skilled person's understanding of certain claim terms.

Prosecution History: Mr. Alexander summarizes portions of the Patent Office files for these patents and explains the relationships between the patents. Included is the Patent Office's statement (set forth with its reasons for allowing the '193 patent to issue) that InterTrust had filed "a series of applications generally relating to a virtual distribution environment."

Deposition Testimony: In opposing Microsoft's motion to stay certain discovery, InterTrust argued that the parties' own uses of the claim terms are important to claim construction. (InterTrust Opp. to Microsoft's Motion for Stay at 9-10 & n. 9 (October 1, 2002).) Microsoft has since deposed several InterTrust employees, former employees, licensees, and licensee candidates, as well as InterTrust's expert, Prof. Reiter. Their testimony confirms that

many key claim terms lack any precise meaning outside of VDE. Ms. Keefe's Declaration collects some of this testimony.

Documentary Evidence: Two Declarations by Xuan-Giang Tran submit documentary evidence supplementing the parties' joint submission of intrinsic evidence.

III. THE BIG BOOK'S "INVENTION"

Microsoft asks the Court to construe each claim as requiring the disclosed "invention," as it has been distilled in Microsoft's global "claim as a whole" construction. (JCCS Exh. A, Row 86). Some of the important aspects of this "invention"—aspects which the Big Book cites to distinguish prior systems—are summarized below. (See also Maier Decl. at 5-14).

Data Security and Commerce World: The overall purpose of the "invention's" Virtual Distribution Environment (VDE) is for securing, administering, and auditing all security and commerce digital information within its multi-node "world." VDE guarantees to all participants in this VDE world that it can limit all access to, and use of, such security and commerce information, to authorized activities and amounts.

> "The **present invention provides a new kind of 'virtual distribution environment' (called 'VDE' in this document) that secures, administers, and audits electronic information use**. VDE also features fundamentally important capabilities for managing content that travels 'across' the 'information highway.'" ('193 2:24-28)
>
> "**The present invention** can provide a "unified," efficient, secure, and cost-effective system for electronic commerce and data security. This allows VDE to serve as **a single standard for electronic rights protection, data security, and electronic currency and banking**." ('193 7:9-14)
>
> "VDE is a cost-effective and efficient rights protection solution that provides a unified, consistent system for securing and managing transaction processing. **VDE can: (a) audit and analyze the use of content, (b) ensure that content is used only in authorized ways, and (c) allow information regarding content usage to be used only in ways approved by content users**." ('193 4:48-55)

(Alexander Decl. Exh. D at 24-1(C), 24-9(C), 24-1(F).) (Emphases added throughout this Brief, unless otherwise noted).

Comprehensive Range of Functions: The Big Book distinguishes its comprehensive "invention" from supposedly "limited" traditional systems that addressed only some aspects of data security and commerce.

> "**Content providers and distributors have devised a number of limited function rights protection mechanisms to protect their rights**. Authorization passwords and protocols, license servers, 'lock/unlock' distribution methods, and non-electronic contractual limitations imposed on users of shrink-wrapped software are a few of the more prevalent content protection schemes. In a commercial context, **these efforts are inefficient and limited solutions.**" ('193 3:1-9)

> "**Despite the attention devoted** by a cross-section of America's largest telecommunications, computer, entertainment and information provider companies **to some of the problems addressed by the present invention, only the present invention provides commercially secure, effective solutions for configurable, general purpose electronic commerce transaction/distribution control systems.**" ('193 2:13-22)

(Alexander Decl. Exh. D at 24-7(K), 24-4(V).)

User-Configurable: The "invention" governs access to and use of protected information with executable VDE "controls." These VDE controls are not built-in, fixed mechanisms. Rather, VDE allows its participants to create, modify, and merge these VDE controls, partly through a VDE-controlled negotiation process. For example, VDE purports to enable[3] a consumer to place limits on the amount of time or money that a participant (whether human or machine) can spend using the protected content, subject only to other users' "senior controls."

> "The **inability of conventional products to be shaped to the needs of electronic information providers and users is sharply in contrast to the present invention.**" ('193 2:11-13)

> "The **configurability provided by the present invention** is particularly **critical for supporting electronic commerce**, that is enabling businesses to create relationships and evolve strategies that offer competitive value. **Electronic commerce tools that are not inherently configurable and interoperable will ultimately fail to produce** products (and services) that meet both basic requirements and evolving needs of most commerce applications." ('193 16:41-48)

---

[3] Throughout this brief, Microsoft describes various features described in the Big Book and other InterTrust patents. By reiterating what InterTrust patent documents say, Microsoft does not imply that those documents actually described a working system that could accomplish what they promised. In other words, Microsoft addresses what the patents purported to describe, not whether they actually enabled anything.

(Alexander Decl. Exh. D at 24-4(V), 24-4(W).)

Flexible: The Big Book further distinguishes its supposedly flexible system from rigid systems. For example, rather than requiring a VDE user to purchase an entire, pre-defined content package (e.g., an entire movie), the "invention" can permit a VDE user to purchase only user-defined increments of that information (e.g., her favorite scenes).

> "**Summary of Some Important Features Provided by VDE in Accordance With the Present Invention.** VDE employs a variety of capabilities that serve as a foundation for a general purpose, sufficiently secure distributed electronic commerce solution. VDE enables an electronic commerce marketplace that supports divergent, competitive business partnerships, agreements, and evolving overall business models. For example, **VDE includes features that . . . support dynamic user selection of information subsets of a VDE electronic information product (VDE controlled content). This contrasts with the constraints of having to use a few high level individual, pre-defined content provider information increments** such as being required to select a whole information product or product section in order to acquire or otherwise use a portion of such product or section. . ." ('193 21:43-53; 22:32-38)

> "**VDE does not require electronic content providers and users to modify their business practices and personal preferences to conform to a metering and control application program that supports limited, largely fixed functionality.**" ('193 9:67-10:9)

(Alexander Decl. Exh. D. at 24-1(Q), 24-10(G).)

The VDE Mechanisms: The Big Book describes various embodiments for providing these (and other) core "invention" capabilities. It describes no embodiment, however, that is said to achieve these "invention" capabilities without using at least the described VDE controls, VDE "secure containers," and VDE "secure processing environments." On the contrary, the Big Book emphasizes that the design of its VDE components is an "Important Feature" of the "invention." (See Alexander Decl. Exh. D at 24-1(S) ('193 21:43-45, 34:25-30).)

None of the above capabilities and components is merely an optional characteristic of some embodiment. They are core, defining features of the "present invention."

IV. THE "INVENTION" PROMISES THAT IT IS ABLE TO PREVENT ALL ACCESS TO AND ALL USE OF PROTECTED CONTENT EXCEPT AS AUTHORIZED BY VDE CONTROLS

Another aspect of the VDE "invention" is particularly important to claim construction.

Non-Circumventable: VDE claims that the protections it promises cannot be bypassed, i.e., they are not circumventable. Rather, VDE intercepts attempts by any and all users (including would be misusers) to access or use protected information. It thereby "ensures" that the VDE controls designed to govern such access and use, in fact do so, and that all unauthorized access and use is "prevented." (See Alexander Decl. Exh. D at 24-5(A), 19(K) ("VDE enables parties ... to ensure that the moving, accessing, modifying, or otherwise using of information can be securely controlled" ('193 6:18-31); "the present invention ensures that content control information can be enforced." ('193 46:4-8).) As stated at '193 11:8-11:

> **"All requirements specified by this derived control information must be satisfied before VDE controlled content can be accessed or otherwise used.**

This non-circumventable "access control" is critical to a proper construction of these patent claims. The secrecy of digital information (e.g., an electronic vote) may be protected by encrypting it. Encryption does not, however, provide full protection. (See Reiter Depo. at 49:7-14, 53:1-11, 55:13-16.) It does not prevent an attacker from deleting the content, or altering it, copying it, tracing it, or moving it. Thus, as the "invention" prevents all types of misuse, it does more than merely encrypt content. Specifically, VDE promises those who entrust their valuable content to it, that VDE is able to prevent all forms of unauthorized access to the content. By preventing unauthorized access, VDE prevents all unauthorized uses, including misuses which are not prevented by mere encryption (such as deleting, altering, copying, or moving the content). In other words, VDE promises a second layer of protection—a bank vault like "access control" that cannot be circumvented:

> "The virtual distribution environment 100 **prevents use** of protected information except as permitted by the "rules and controls" (control information). ('193 56:26-28)

> "As mentioned above, virtual distribution environment 100 'associates' content with corresponding 'rules and controls,' and **prevents the content from being used or accessed** unless a set of corresponding 'rules and controls' is available." ('193 57:18-22)

> "Although block 1262 includes encrypted summary services information on the back up, it preferably does not include SPU device private keys, shared keys, SPU code and other internal security information **to prevent this information from ever becoming available to users even in encrypted form.**" ('193 166:59-64)

InterTrust's expert, Prof. Reiter, has agreed that the '193 Patent says that VDE is able to prevent physical access to protected content. (See Reiter Depo. at 55:17-60:1). Nevertheless, InterTrust's proposed constructions uniformly disregard this core VDE promise.

This "access control" capability of the "invention" is critical to a proper understanding of the most important claim terms in dispute. For example, various claims promise protections against unauthorized "use" or "copying" of protected content. InterTrust's proposed constructions of "use" and "copy" assume that only encryption is used to protect the content. Thus, per InterTrust, "use" and "copy" must mean only those types of uses and copying which can be prevented with encryption. That construction is wrong because that assumption is wrong. VDE promises content access control, not just encryption. In this VDE context, the claims protect against all forms of use and copying, not just those which require decryption.

V. CLAIMS CONSTRUCTION LAW

A. General Claim Construction Legal Analysis

The statutory measure of a patent's scope is its patented "invention," which is required to be set forth "distinctly" in the patent claims. 35 U.S.C. § 112, ¶ 2. There are statutory requirements to help ensure that what is claimed is the "invention." One is that a patent may claim as its invention only subject matter that "the applicant regards as his invention." 35 U.S.C. § 112, ¶ 2. Another is that a patent may claim only the "invention" described in the patent application's written description. 35 U.S.C. § 112, ¶ 1. These requirements, coupled with the public notice function of a patent, explain why it is fundamental that "claims are to be construed in the light of the specifications and both are to be read with a view to ascertaining the **invention**." Adams, 383 U.S. at 49; see also Vitronics Corp. v. Conceptronic, Inc., 90 F.3d 1576 (Fed. Cir. 1996) ("the public is entitled to rely" on the instrinsic evidence for notice as to what the patent does and does not cover). Last year the Supreme Court confirmed this necessary link: "What is claimed by the patent application must be the same as what is disclosed in the specification." Festo, 535 U.S. at 736 .

The standard claim construction rules are set forth in Vitronics. See 90 F.3d at 1582-83 (citing Markman v. Westview Instrs., Inc., 52 F.3d 967 (Fed. Cir. 1995), aff'd, 517 U.S. 370

(1996)). See also Schering Corp. v. Amgen Inc., 222 F.3d 1347, 1353 (Fed. Cir. 2000) (interpreting patent terms as one of skill in the art at the time of the application would understand them). In ascertaining the patent's "invention," the claims' language is of primary importance. See Vitronics, 90 F.3d at 1582. However, courts must look also to both "intrinsic" and "extrinsic" evidence. See Lacks Indus. v. McKechnie Vehicle Components USA, Inc., 2003 U.S. App. LEXIS 4471, at *14 (Fed. Cir. Mar. 13, 2003) (for claim construction, "we begin with an examination of the intrinsic evidence, i.e., the claims, the other portions of the specification, and the prosecution history (if in evidence). Courts may also review extrinsic evidence in construing a claim. Additionally, dictionary definitions, although extrinsic, may be used to establish a claim term's ordinary meaning.") (internal citations omitted) (See Tab B, hereto).

Among the intrinsic evidence, "the specification is always highly relevant to the claim construction analysis. Usually, it is dispositive; it is the single best guide to the meaning of a disputed term." Vitronics, 90 F.3d at 1582.[4] "One purpose for examining the specification is to determine if the patentee has limited the scope of the claims." Watts v. XL Sys., Inc., 232 F.3d 877, 882 (Fed. Cir. 2000). In making this determination, however, courts must refrain from reading in unnecessary limitations from the specification into the claims. See Comark Communications, Inc. v. Harris Corp., 156 F.3d 1182, 1186 (Fed. Cir. 1998).

Recent Federal Circuit decisions have proposed that a way to help ensure this balance is to first look to the "ordinary meaning" of claim terms, then review the specification and prosecution history to ensure that it is appropriate to apply the "ordinary meaning." See Texas Digital Sys., Inc. v. Telegenix, Inc., 308 F.3d 1193, 1201-04 (Fed. Cir. 2002) (construing, *inter alia*,

---

[4] InterTrust's brief erroneously implies that a patent specification's purpose is limited to providing an enabling disclosure. (InterTrust Br. at 4:17-18). However, Federal Circuit precedent makes clear that even when the claims are plain on their face, it is necessary to consult the specification during claim construction. See Prima Tek II, L.L.C. v. Polypap, S.A.R.L., 318 F.3d 1143, 1148 (Fed. Cir. 2003) ("After identifying the plain meaning of a disputed claim term, the court examines the written description and the drawings to determine whether use of that term is consistent with the ordinary meaning of the term."); Texas Digital Sys., Inc. v. Telegenix, Inc., 308 F.3d 1193, 1204 (Fed. Cir. 2002) ("the intrinsic record also must be examined in every case").

"activating" in accordance with the ordinary meaning, consistent with the intrinsic evidence, and not accepting patentee's broader proposed construction). Under this approach, the first challenge is to determine whether there is an "ordinary meaning." Id. To do so, courts look to the plain language of the claims and determine whether **appropriate** dictionaries or treatises provide guidance as to the meaning of the terms. See id. at 1202-04; cf. Hoechst Celanese Corp. v. BP Chems. Ltd., 78 F.3d 1575, 1580 (Fed. Cir. 1996) ("a general dictionary definition is secondary to the specific meaning of a technical term as it is used and understood in a particular technical field."). Courts then "must" examine the intrinsic record to ensure consistency with the "ordinary" meaning; "[i]ndeed, the intrinsic record may show that the specification uses the words in a manner clearly inconsistent with the ordinary meaning . . . [and, in such a case, the "ordinary meaning"] must be rejected." Texas Digital, 308 F.3d at 1204. The intrinsic record may also be used to select from among various "ordinary meanings." Id. at 1203. Cf. Rexnord Corp. v. Laitram Corp., 274 F.3d 1336, 1345 (Fed. Cir. 2001) (observing that the "Summary of the Invention" section of the written description is "a pertinent place to shed light upon what the patentee has claimed.").

In certain instances, a "plain meaning" simply does not exist. See, e.g., Lacks, 2003 U.S. App. LEXIS at *16 ("the dictionary definitions do not provide a plain meaning"); J.T. Eaton & Co. v. Atlantic Paste & Glue Co., 106 F.3d 1563, 1568 (Fed. Cir. 1997) (disputed claim term "is a term with no previous meaning to those of ordinary skill in the prior art. Its meaning, then, must be found somewhere in the patent.").

Even where an ordinary meaning exists, there are several situations in which the Federal Circuit has recognized that the "ordinary meaning" is not appropriate. See, e.g., CCS Fitness, Inc. v. Brunswick Corp., 288 F.3d 1359, 1366 (Fed. Cir. 2002) ("a court may constrict the ordinary meaning of a claim term in at least one of four ways"). Significant precedent establishes at least the following ways, relevant to the claims in this mini-Markman proceeding, in which claim terms should not be afforded their "ordinary meaning":

1) **To Provide Clarity**: A claim term will not have its ordinary meaning **if the term "chosen by the patentee so deprive[s] the claim of clarity" as to require resort to the other**

intrinsic evidence for a definite meaning." Altiris, Inc. v. Symantec Corp., 318 F.3d 1363, 1374-75 (Fed. Cir. 2003) (holding that "automation code" "is so broad as to lack significant meaning" and, thus, court limited claim to the only disclosed embodiment). See generally NeoMagic Corp. v. Trident Microsystems, Inc., 287 F.3d 1062, 1071-72 (Fed. Cir. 2002) (restricting claim to a particular type of electrical "coupling," based on specification, although dictionary definition was more general); Watts, 232 F.3d at 882-83 (holding claim term was not "clear on its face," and limiting the claim to a particular embodiment which was described as a feature of the "present invention"); Ethicon Endo-Surgery, Inc. v. U.S. Surgical Corp., 93 F.3d 1572, 1579 (Fed. Cir. 1996) (limiting "pusher assembly" to that described in drawings when the term was "ambiguous" and the specification provided "minimal guidance"); North Am. Vaccine, Inc. v. American Cyanamid Co., 7 F.3d 1571, 1576 -77 (Fed. Cir. 1993) (limiting unclear claim term "linkage to a terminal portion" to linkage at only one terminal as described in the specification).

2) Express or Implied Definition in Patent: "[T]he claim term will not receive its ordinary meaning if the patentee acted as his own lexicographer and **clearly set forth a definition of the disputed claim term in either the specification or prosecution history.**" CCS Fitness, 288 F.3d at 1366-67 (citing Johnson Worldwide Assoc. v. Zebco Corp., 175 F.3d 985, 990 (Fed. Cir. 1999); Rexnord Corp. v. Laitram Corp., 274 F.3d at 1342). The patent applicant's definition need not be express; when a patentee uses a claim term throughout the entire patent specification, in a manner consistent with only a single meaning, he has defined that term "by implication." Bell Atlantic Network Servs., Inc. v. Covad Communications Group, Inc., 262 F.3d 1258, 1268, 1273 (Fed. Cir. 2001) (limiting claim term "mode" to one type of mode, as the patent "defined the term 'mode' by implication" throughout the specification). See generally Abbot Labs. v. Novopharm Ltd., 2003 U.S. App. LEXIS 5357, at **13-18 (Fed. Cir. Mar. 30, 2003) (construing "a co-micronized mixture of particles of [x and y]" to mean "co-micronization of a mixture consisting essentially of only [x and y]" based on definition provided in specification) (emphasis in original) (See Tab A, hereto); Multiform Desiccants, Inc. v. Medzam, Ltd., 133 F.3d 1473,

1477-78 (Fed. Cir. 1998) (observing that an inventor may bestow "a special meaning to a term in order to convey a character or property or nuance relevant to the particular invention").

3) Important to "Invention": The court will limit the ordinary meaning where the specification describes a particular feature or embodiment as **"important to the invention."** E.g., Toro Co. v. White Consol. Indus., 199 F.3d 1295, 1301 (Fed. Cir. 1999) (limiting claim term to a unitary structure based in part on statements in the specification describing that structure as "important to the invention"). Cf. Scimed Life Sys. v. Advanced Cardiovascular Sys., 242 F.3d 1337, 1342-43 (Fed. Cir. 2001) (limiting claim term "lumen" to "coaxial lumen" in part because the specification characterized the coaxial configuration as part of the "present invention.")

4) Distinguishing Prior Art: "[A] claim term will not carry its ordinary meaning if the intrinsic evidence shows that the **patentee distinguished that term from prior art on the basis of a particular embodiment,"** CCS Fitness, 288 F.3d at 1366-67 (citing Spectrum Int'l Inc. v. Sterilite Corp., 164 F.3d 1372, 1378 (Fed. Cir. 1998) (narrowing a claim term's ordinary meaning based on statements in intrinsic evidence that distinguished claimed invention from prior art). See generally Rheox, Inc. v. Entact, Inc., 276 F.3d 1319, 1325-26 (Fed. Cir. 2002) (restricting claim to a particular type of phosphate in light of prosecution history disclaimer of other types of phosphate, despite specification's description of some of the "disclaimed" types of phosphate); Innovad Inc. v. Microsoft Corp., 260 F.3d 1326, 1332 (Fed. Cir. 2001) (restricting claim to devices that did not have keypads, based on specification and prosecution history statements distinguishing prior art).

5) Express Disclaimer: A claim term will not carry its ordinary meaning if the intrinsic evidence shows the patentee **"expressly disclaimed subject matter."** CCS Fitness, 288 F.3d at 1366-67. See generally Scimed, 242 F.3d at 1342-44 (limiting claim term based in part on statements in the specification indicating the invention "excludes" other structures); Ballard Med. Prods. v. Allegiance Healthcare Corp., 268 F.3d 1352, 1361-62 (Fed. Cir. 2001) (finding an explicit disclaimer of "pressure valves" and "dynamic seals" where patentee asserted that his invention, in contrast to such prior art, comprised "vacuum valves" and "static seals").

As shown above, District Courts, the Federal Circuit, and the Supreme Court frequently determine the scope of the "invention" described in the patent specification in the course of determining scope of the issued claims. Where there is a possible disconnect between the disclosed "invention" and the claims, the Federal Circuit normally will construe the claims narrowly, rather than invalidate the claims. See, e.g., Tate Access Floors, Inc. v. Interface Architectural Res., Inc., 279 F.3d 1357, 1367 (Fed. Cir. 2002) ("claim language should generally be construed to preserve validity, if possible"); Schering Corp., 222 F.3d at 1353-54 (limiting claim to one subspecies, as that was all that was described and enabled by specification). However, where the claim on its face is clear and there is no link or "hook" at all in the claim for what the patent described as the "invention," then the Court may construe the claim broadly, but invalidate it under Sec. 112, ¶ 2 or ¶ 1. See, e.g., Cardiac Pacemakers, Inc. v. St. Jude Med., Inc., 296 F.3d 1106, 1114 (Fed. Cir. 2002) ("where the specification fails to disclose structure corresponding to the claimed function, [preserving validity] is impossible [so] the claims are invalid."); Tate Access, 279 F.3d at 1372 ("where claim language is clear we must accord it full breadth even if the result is a claim that is clearly invalid.").

B. Other Claim Construction Issues In This Case

1. Incorporation f One Pending Application Into Another By Reference

Three InterTrust patents (the '683, '721, and '861) purport to incorporate the Big Book by reference to the unpublished patent **application**. (See '721 at 1:7-19; '683 at 1:11-23; '861 at 1:7-11.) However, the specifications of these three patents were never amended to properly reference the Big Book's issued patent number, as required by the Patent Office. See In re De Seversky, 474 F.2d 671 (C.C.P.A. 1973); Manual of Patent Examining Procedure § 608.01(p). This failure means that the Big Book is not part of the "specifications" of these three patents. Nonetheless, the Big Book remains intrinsic evidence for the '683 Patent (as it is in that patent's prosecution history) and extrinsic evidence for the others.

2. Restriction Requirements and Divisional Patent Applications

InterTrust argues that a Patent Office restriction requirement "conclusively rebuts"

Microsoft's position that the Big Book is drawn to a comprehensive VDE "invention." InterTrust's argument misses the mark for several reasons.

First, the claim construction point being made by Microsoft is that all of these claims necessarily invoke the required "features" of the VDE "invention," not that all claims require only those features. InterTrust's patent claims are free to recite additional features, which additional limitations may (or may not) make them separate "inventions" under Patent Office restriction practice. But, that is not the issue here.

Moreover, in entering the restriction requirement, the Patent Office did not indicate that it was construing the claims as non-VDE claims, requiring none of the required features of the disclosed "invention." Rather, the Patent Office merely grouped the original claims of the "Big Book" application into different categories that were supposedly "related as subcombinations disclosed as usable together in a single combination." (InterTrust Brief at 11 (citing September 25, 1996, Office Action at 2-3.) InterTrust admits in its opening brief that Rambus Inc. v. Infineon Techs., 318 F.3d 1081 (Fed. Cir. 2003), is distinguishable because none of the restriction requirements here specifically involved the VDE limitations, whereas in Rambus the limitation at issue was directly involved in the restriction requirement. (InterTrust Br. at 13, n. 7).

Also, that a restriction requirement was made does not mean that subsequent claims are directed to separate inventions. Rather, a court must closely scrutinize the scope of claims issuing from a divisional application. Gerber Garment Tech., Inc. v. Lectra Sys., 916 F.2d 683, 688 (Fed. Cir. 1990) (invalidating divisional claims for double patenting, because applicant had amended such that they were no longer distinct inventions). Here, as in Gerber, the claims at issue were changed from the original application claims that "spun off" after the restriction requirement. (Alexander Decl., ¶¶ 17.) Consequently, any "presumption" that these issued claims are directed to a different "invention" should not apply.

Finally, courts have limited claims based on descriptions in the specification, despite the fact that a patent issued from a "divisional" application. See Ballard, 268 F.3d at 1360-62 (Fed. Cir. 2001) (limiting claims of both a patent issued from the parent application and a patent issued

from a divisional of such parent to exclude a particular type of valve based on statements made in common specification text and prosecution history of the parent application).

3. Claim Terms Are Construed Consistently in Related Patents

InterTrust incorrectly asserts that "divisional" patents should be separated from their parent. On the contrary, related patents should be construed consistently. Specifically, terms in patent families should generally be afforded the same construction. See AbTox, Inc. v. Exitron Corp., 131 F. 3d 1009, 1001 (Fed. Cir. 1997), amending on reh'g 122 F.3d 1019 (Fed. Cir. 1997) ("Although these claims have since issued in separate patents, it would be improper to construe this term differently in one patent than another, given their common ancestry.") Also, limitations set forth in one patent's specification or prosecution history, may act as a limitation on the related patents. Elkay Mfg. Co. v. Ebco Mfg. Co., 192 F.3d 973, 980 (Fed. Cir. 1999) ("When multiple patents derive from the same initial application, the prosecution history regarding a claim limitation in any patent that has issued applies with equal force to subsequently issued patents that contain the same claim limitation"); see also Mark I Mktg. Corp. v. R.R. Donnelley & Sons Co., 66 F.3d 285, 291 (Fed. Cir. 1995) (restricting claim scope based on prosecution of "grandparent" application).

VI. EACH OF THE TWELVE CLAIMS SHOULD BE CONSTRUED TO REQUIRE THE DISCLOSED "INVENTION"

A. '193, Claims 1, 11, 15, 19

The '193 Patent publishes the Big Book specification without any substantive additions (and thus is cited throughout this Brief as a surrogate for the Big Book).

Contrary to InterTrust's position (InterTrust Br. at 8:9-10), all four '193 Patent mini-Markman claims concern the distribution and protection of digital content, and contemplate multiple nodes and participants. Information is received (possibly from multiple upstream content providers), then stored on a device having unspecified authorized and unauthorized users, and then conditionally transferred to another device having unspecified users. The claims promise to control three forms of unauthorized use of this distributed content: copying, distributing (to the second device), and storing (on the first and/or second device):

"if said copy control allows at least a portion of said digital file to be copied and stored on a second device…." ('193 321:10-11)

"determining" or "determine" "whether said digital file may be copied and stored on a second device …." ('193 321:7-9)

This claim language (e.g., "if … allows," "determining whether") is not qualified. It implies that if the copying and storing are not allowed, then they are prevented (see Reiter Depo. at 174:1-178:11), no matter what effort may be made to take the unauthorized action. In other words, these claims imply that their "controls" are effective in the face of the attacks identified in the Big Book.

These claimed protections against misuse cannot be achieved by encrypting the content. Encryption would not prevent the content from being accessed, copied, distributed, or stored. For these types of protection, "access control" is necessary. More particularly, the Big Book describes only the complete "invention" as providing such protection against the threats identified in the Big Book. In other words, by promising the type of effective access control protection said to be provided only by the complete VDE, these claims invoke that "invention." Their use of the vague, VDE term "control" also invokes the "invention."

B. '683, Claim 2

The '683 Patent is a "continuation-in-part" (CIP) which does not contain the Big Book's text. Although it purports to incorporate the Big Book, it fails the Patent Office's rules for incorporating "essential matter." (See supra, V. B.1 at 14.) Nevertheless, the Big Book is part of this patent's prosecution history, and thus is intrinsic evidence for claim construction purposes.

This claim also concerns a multi-node distribution system. Here, "secure containers" and "secure container rules" are distributed amongst various nodes. The claim appears to promise the ability to prevent access to or use of protected information, using the secure containers, secure container rules, and a "protected processing environment." (See Second Mitchell Decl. at 6-7.) These protections are not qualified as to the nature or severity of the threat being faced; they impliedly are effective against all threats identified in the patent or Big Book. The only system described in the Big Book or '683 Patent said to accomplish such protections, is the complete

VDE. This claim further invokes VDE by using VDE and vague terminology, such as "secure container" and "protected processing environment."

C. '721, Claims 1, 34

The '721 Patent neither contains the Big Book, nor incorporates it in the manner required by the Patent Office for incorporating essential matter into a patent. Moreover, the Big Book is not in the '721 Patent's Patent Office prosecution history. Thus, the Big Book is merely extrinsic evidence for purposes of construing these claims.

The '721 Patent purports to improve the Big Book VDE by preventing the use of executable code (specifically, "load modules" in Claim 1) except as authorized. Such prevention requires an access control capability. Claims 1 and 34 promise such protections without any qualification that they are effective only sometimes, or in some situations. Neither the Big Book nor the '721 Patent describes anything other than a full VDE system for achieving these types of promised results in the face of the threats identified in those documents. These claims further invoke the "invention" by reciting several terms that invoke VDE for context, including "protected processing environment," "tamper resistant barrier," and "security."

D. '861, Claim 58

The Big Book also is merely extrinsic evidence for purposes of construing this claim.

This patent discusses a possible attack on the "security" of "secure containers." It requires that the process of creating VDE secure containers be itself protected. ('861 4:51-64)

Claim 58 recites such a method for creating secure containers. It appears to promise the ability to prevent any access to or use of certain information (by putting the information in a secure container), except as authorized by a rule. It also provides a particular rule designed to control at least one aspect of allowed use or access. Again, the promised protection is not qualified by type or severity of threat. Neither this patent nor the Big Book describes any non-VDE system for achieving this promised capability. This claim further invokes VDE by reciting various vague and VDE terms, including "secure container" and "control."

E. '891, Claim 1

This patent publishes the Big Book without addition.

This claim appears to make the unqualified promise that it prevents an appliance from using content protected by controls received from two remote entities, except as authorized by those controls. This ability to prevent all use implies an ability to control access. Again, the patents describe no non-VDE system having this capability. This claim also uses several vague and VDE terms, such as "secure operating environment," "securely receiving," "control," "securely processing," and "securely applying."

F. '900, Claim 155

This patent repeats the Big Book, but also adds to it. It addresses various possible attacks against VDE's protections, including one in which a VDE's foundation software (which, e.g., runs to create a VDE "host processing environment") is copied onto another machine to form a rogue VDE node. ('900 233:8-15). One of the solutions described in this patent is to embed a unique identifier, called a "machine signature," into the VDE software so that it cannot run on a different machine. ('900 237:40-54, 239:5-14).

Claim 155 recites a method using "machine check programming" for checking a VDE host processing environment and halting processing. This method also is unqualified, i.e., it does not rule out any of the types or severities of threat described in this patent. Also, it uses several VDE specific or otherwise vague terms, such as "virtual distribution environment," "host processing environment," "machine check programming," and "tamper resistant software," which need to be clarified and construed in light of the VDE "invention."

G. '912, Claims 8, 35

This patent is a "divisional" patent which publishes the Big Book without change.

These claims are somewhat similar to those of the '721 Patent. Claim 8 appears to promise the ability to prevent use of a load module within an execution space, except as authorized. Claim 35 appears to promise the unqualified ability to prevent use of certain "specified information," in part by protecting the process of creating the "component assembly" which controls that use. By preventing unauthorized uses, each claim implies an access control capability. Again, the Big Book describes no non-VDE system with this unqualified capability. These claims also use several VDE or vague terms, such as "component assembly," "load

module," "level of security," "securely assembling," and "secure container."

In sum, had these twelve claims used only precise, well-defined, non-VDE terminology, and not promised the types and levels of protection provided by VDE, then they might not have invoked the disclosed "invention." That, however, is not the case.

VII. CONSTRUCTION OF THE CLAIM TERM "USE"

Central Dispute: Whether an encrypted file may be "used" without decrypting it.

As explained above, VDE prevents all forms of unauthorized "use" of protected information, including forms of misuse which do not require decryption, such as deleting or altering someone else's encrypted content.

Ordinary Meaning: Microsoft's construction follows from the ordinary, everyday meaning of "use." A "use," of course, may be a "misuse." In "security" systems, the most important uses to address are the potential misuses, including those by unauthorized users. Microsoft's construction does that, and includes several uses which may be misuses (such as deleting someone else's data).

Microsoft's Construction: "(1) To use information is to perform some action on it or with it (e.g., copying, printing, decrypting, encrypting, saving, modifying, observing, or moving, etc.)…." (JCCS Exh. A at Row 42).

This is precisely how the term "use" is used in the Big Book and '683 Patent:

> "These appliances typically include a secure subsystem that can enable control of **content use such as displaying, encrypting, decrypting, printing, copying, saving, extracting, embedding, distributing, auditing usage**, etc." ('193 9:24-27)
>
> "In general, VDE enables parties that (a) have rights in electronic information, and/or (b) act as direct or indirect agents for parties who have rights in electronic information, to ensure that **the moving, accessing, modifying, or otherwise using of information** can be securely controlled by rules regarding how, when, where, and by whom such activities can be performed." ('193 6:24-31)
>
> "Provides non-repudiation of use and may record specific **forms of use such as viewing, editing, extracting, copying, redistributing (including to what one or more parties), and/or saving.**" ('683 6:46-48)

(Alexander Dec. Exh. D at 23(G), 23(C), 23(A).) Nothing in these patents counters these Big

Book definitions of "use" as including copying, encrypting, saving, modifying, and moving.

Importantly, many of these actions which the Big Book refers to as "uses" cannot be blocked by encryption and, conversely, require no decryption of the content to perform. That such uses are indeed "uses," is further confirmed by the parties' agreed definition of "tampering" (which includes "altering" within "use" (see JCCS Exh. I at Row 8)), and InterTrust's proposed definition of "VDE" (which includes "distribution" within "use" (see JCCS Exh. A at Row 86)).

Microsoft's proposed construction further requires that "(2) In VDE, information Use is Allowed only through execution of the applicable VDE Control(s) and satisfaction of all requirements imposed by such execution." (See JCCS Exh. A at Row 42). This is VDE's "prevent unauthorized use" protection mechanism, governed by VDE controls, which is found throughout the Big Book, and explained by Prof. Maier (Maier Decl. at 7-8, 38-41).

InterTrust's Proposed Construction: InterTrust's proposed construction of "use" is typical of most of its constructions: short, unclear, and contrary to the Big Book: "to put into service or apply for a purpose, to employ." (See JCCS Exh. A at Row 42). This loose language may be fine as a general concept, but is not adequate for a claim construction. It does not clearly or precisely define the types of use (e.g., misuses) of digital information it encompasses or excludes. On the contrary, it would leave the jury and public guessing about which of the following actions, **expressly identified as "uses" in the patents**, are "uses": copying, encrypting, saving, modifying, and moving.

InterTrust apparently contends that nothing is a "use" of information if it cannot be prevented by encryption alone. In other words, if content is encrypted, a "use" of that information must require decryption, or else it is not a "use." Per InterTrust, apparently, none of these Big Book uses, is a use: deleting content, altering it, saving it, encrypting it, copying it, or moving it.

This position is contrary to the Big Book's above-quoted express statements that "use" includes deleting, saving, encrypting, moving, and copying. More importantly, it is contrary to the core promise of the VDE "present invention" that its access control capabilities can prevent all unauthorized access to and use of protected content, not just those uses which could be

blocked through encryption.

The Court should expressly include within "use" all of those actions expressly identified as "uses" in the Big Book and the '683 Patent, as set forth in Microsoft's construction.

VIII. CONSTRUCTION OF THE CLAIM TERM "COPY"

Central Dispute: Whether a reproduction is still a "copy" if it is unusable or inaccessible to someone.

Ordinary Meaning: Under its ordinary meaning, to "copy" something is to reproduce it, and the resulting reproduction is a "copy." The copy, of course, remains a copy even if it is locked away and inaccessible. It also remains a copy if given to someone who cannot use it.

Microsoft's Construction: "(1) To reproduce all of a Digital File or other complete physical block of data from one location on a storage medium to another location on the same or different storage medium, leaving the original block of data unchanged, such that two distinct and independent objects exist. (2) Although the layout of the data values in physical storage may differ from the original, the resulting "copy" is logically indistinguishable from the original. (3) **The resulting "copy" may or may not be encrypted, ephemeral, usable, or accessible.**" (See JCCS Exh. A at Row 5).

This is how the Big Book uses the term "copy." A copy of an encrypted electronic file is still a copy even when possessed by someone who has no right to decrypt it or otherwise use it. Thus, the Big Book refers to a reproduction of a video program as a "copy" even though its recipient cannot watch or copy it: "Even if a consumer has a **copy of a video program**, she cannot watch or copy the program unless she has "rules and controls" that authorize use of the program." ('193 53:60-62). On the other hand, when the Big Book means a copy which is usable, it says so: "For example, if a software program was distributed as a traveling object, a user of the program who wished to supply it or a **usable copy** of it to a friend would normally be free to do so." ('193 131:65-132:1). (Alexander Dec. Exh D at 10(C)-10(E).)

InterTrust's expert, Prof. Reiter, has testified that this everyday "reproduction" sense of the word "copy," in which a copy is still a copy even if possessed by someone who cannot

decrypt it, is "a very common use of the word 'copy.'" (Reiter Depo. at 64:12-65:8, 66:1-15)). He also has conceded that the Big Book used the term "copy" in this manner in the above "video program" quote, and elsewhere. (Reiter Depo. at 68:5-70:7, 74:21-75:17).

InterTrust's Proposal: Despite this usage in the Big Book and these concessions of its expert, InterTrust nevertheless urges the Court to dismiss this "very common" usage and construe "copy" as if a copy is no longer a copy when locked away or given to someone who cannot decrypt it. Rather than expressly say so, however, InterTrust says merely that "the reproduction must be useable." (See JCCS Exh. A at Row 5). As interpreted by its expert, Prof. Reiter, InterTrust does not here mean "usable" in the VDE sense of "use" (described above). Rather, by "must be usable," InterTrust apparently means that a reproduction of encrypted content is not a copy when possessed by someone who cannot decrypt it. In other words, whereas the '193 claims expressly limit the number of "copies" which can be made, InterTrust urges the Court to read these claims as if they limit the number of "decryptable (by present holder) copies." InterTrust's proposal is unworkable, contrary to the specification's use of "copy," and wholly divorced from the core VDE "prevent unauthorized access" capability.

Unworkable: Under InterTrust's apparent theory, a non-copy would become a copy when handed to someone who can decrypt it, and then become a non-copy again when handed back. Such a vacillating status as "copy" is not workable. How can a system "control copying," if the reproduction's status as a "copy" depends on who happens to possess it in the future?

Contrary to Specification: The Big Book not once suggests that a "copy" **must** be decryptable or "usable." On the contrary, as noted above, the Big Book focuses on ways to **prevent** use (e.g., misuse) of files and copies; expressly states that one needs appropriate controls to use a "copy" ('193 53:60-63); and refers to a "usable copy" to indicate that controls allow the copy to be used ('193 131:67). Indeed, Prof. Reiter agreed that InterTrust's proposed construction of "copy" was inconsistent with the above-quoted Big Book's use of the term "copy" in connection with a video program. (Reiter Depo. at 71:19-73:17).

Contrary to the VDE "No Unauthorized Access" Promise: Perhaps most importantly, in its construction of "copy," InterTrust again ignores and contradicts the VDE "present invention."

These claims concern copying not only by authorized end-users, but also by unauthorized mis-users. Preventing such unauthorized copying, even by someone who is unable to decrypt those copies, is an important "security" feature. For example, unauthorized copying of encrypted files can be used as a "denial of service attack" on a computer system by replicating the encrypted files into a computer's memory to deny legitimate access to that memory by authorized users. (This attack is especially effective if the files are written to a write-only medium.) Or, an attacker could copy multiple encrypted files to his own computer to study the encryption scheme. In neither of these examples was the attacker authorized to decrypt the encrypted "copy," but he nevertheless was able to use copying of encrypted files for his own unauthorized purposes. (See Second Mitchell Decl. at 6-7 (discussing "copy").)

The claimed methods can block all unauthorized copying because VDE supposedly is able to block all access to the encrypted content. InterTrust's position wrongly assumes that only the ability to decrypt content is being controlled. In other words, by arguing that a "copy" is not usable if it cannot be decrypted (and thus is not a copy), InterTrust is trying to transform this claim which prevents all unauthorized copying (i.e., has at least two levels of protection), into a claim which merely prevents unauthorized decryption of copies (i.e., has only one level of protection).

Other Disputes Over This Term: One, of course, may copy all of something or only a portion. InterTrust argues that copying a portion of a file can be referred to as copying the file, while Microsoft submits that copying a portion is just that, copying a portion. If a claim speaks of copying a file, it means copying the entire file. When the claims, and patents, mean to refer to a portion, they say "portion." (Compare '193, Claim 1 ("copying at least a portion of said digital file"), with '193 Claim 11 ("determining whether said digital file may be copied."))

InterTrust also argues that "copying" includes altering something, "as long as the essential nature of the content remains unchanged." (See JCCS Exh. A at Row 5). That is unsupported by the patents, and unworkably vague.

IX. CONSTRUCTION OF "SECURE"; "SECURELY"

Central Dispute: Whether a "secure" condition is one in which the threats identified in the patents are prevented, rather than one in which, e.g., some form of attack is detected (but not prevented).

Ordinary Meaning: It is well recognized in computer science that "secure" is a label for an achieved condition or state of being:

> "**State achieved** by hardware, software or data **as a result of successful efforts** to prevent damage, theft or corruption," (Spencer, 156; see Reiter Depo.at 221:4-7) (cited by InterTrust for another term)
>
> "Security is a negative attribute. **We judge a system to be secure if we have not been able to design a method of misusing it** which gives some advantage to the attacker." (Davies, p. 4)
>
> "Definition 4-1. A *security policy* is a statement that partitions the states of the system into a set of *authorized*, or *secure*, states and a set of *unauthorized*, or *nonsecure*, states . . . Definition 4-2 A ***secure system*** **is a system that starts in an authorized state and cannot enter an unauthorized state.**" (Italics in original) (Bishop, p. 95)

(Alexander Dec. Exh. D at 19(JJ), 19(XX), 19(TT).) (See also Reiter Depo. at 30:11-34:5, 35:9-36:18, 222:11-223:1.)

As explained in Prof. Mitchell's first Declaration, there are myriad flavors and degrees of being "secure," depending on a host of contextual variables, such as what is being protected, against what, for how long, to what degree, etc. The patents confirm this by using "secure" to mean different things in different places. The unanswerable question is what does "secure" mean in these context-light claims? (See Microsoft's Motion for Summary Judgment on Indefiniteness).

InterTrust's Proposed Construction: InterTrust's proposed construction of "secure" is so extreme that we address it first: "One or more mechanisms are employed to prevent, detect or discourage misuse of or interference with information or processes. Such mechanisms may include concealment, Tamper Resistance, Authentication and access control. Concealment means that it is difficult to read information (for example, programs may be encrypted). Tamper Resistance and Authentication are separately defined. Access control means that Access to

information or processes is limited on the basis of authorization. Security is not absolute, but is designed to be sufficient for a particular purpose." (See JCCS Exh. A at Row 3).

"One or more mechanisms are employed ....": InterTrust's construction is contrary to the ordinary meaning of "secure" in many respects. First, being "secure" is like being "intelligent" or "beautiful;" it is a condition or a state of being. It is not a statement that some effort was made to become secure (or intelligent or beautiful); it is a label confirming a successful result. For example, placing a combination lock on a safe "employs" a security "mechanism," but that does not mean that the safe is "secure" (e.g., the combination might be easy to guess, or even posted on the safe; the safe's door might be left unlocked, or the safe's walls might easily be broken, etc.).

InterTrust's proposed construction is wrong in this very basic respect. It says that something is "secure" if some effort is made: the result doesn't matter. That is illogical, contrary to the ordinary meaning, and contrary to the Big Book's promises that VDE's security mechanisms can achieve a truly secure environment.

"To prevent, detect, or discourage ....": This is another example of how far InterTrust is willing to distance the claims from the VDE "present invention." Whereas the VDE invention promises the ability to **prevent** all access, use, observation, and interference with protected content, InterTrust would have the Court rule that something is "secure" even if its content is easily destroyed, copied, distributed, and read by others, so long as the system "detects" or "discourages" this misuse. Detecting misuse can be an important function that helps achieve a secure condition, but detecting alone, without preventing misuse, is not security.

Indeed, that InterTrust would urge that a "secure" container, environment, space, memory, etc., may not prevent (or even discourage) any threat whatsoever, no matter how weak the attack, illustrates how flawed its whole approach to claim construction has been. Claim construction is not a word game where one hunts for bits and pieces of definitions from dictionaries written without the "invention" in mind, and tries to fit them together to get the broadest and vaguest possible meaning of a claim term. Rather, as the Patent Statutes require, the Supreme Court has held, and the Federal Circuit has recognized, "what is claimed by the patent application must be the same as what is disclosed in the specification."

<u>"Such mechanisms may include concealment, Tamper Resistance, Authentication and access control."</u>: Prof. Reiter has testified that, under InterTrust's proposal, the term "secure" **does not require any** of these listed forms of protection. (Reiter Depo. at 201:14-204:14). This, again, is at odds with the Big Book's promise that VDE prevents all unauthorized access, use, observation, and interference.

<u>"Security is not absolute, but is designed to be sufficient for a particular purpose"</u>: This statement points out a basic problem with the use of "secure" in these claims and with InterTrust's proposed construction. As with "intelligence," being "secure" is a multi-dimensional, subjective characteristic for which some objective criteria is necessary if skilled evaluators are to objectively determine whether or not something is "secure." That the term "secure" is used in the specification to refer to different things in different contexts, as InterTrust notes, only confirms why context is all important to an understanding of what the term means in the claims. Neither these claims, nor InterTrust's "sufficient for a particular purpose" proposal, however, provides such context or any objective criteria for evaluating what is or is not "secure."

The "designed to be" language of InterTrust's proposed definition language hints that, in InterTrust's view, the "purpose" necessary for evaluating whether something is secure can be gleaned not from the patents, but from the "designer" of an individual accused system or components. That makes no sense. Assume that A and B design two identical systems, each with a different "purpose" in their designs. C acquires these identical systems and offers them to a potential customer D who first wants to know whether these two identical systems are "secure" as meant in these patent claims. It simply cannot be true that one system is "secure" while the other identical system is not (because of the different purposes of their designers). Rather, the necessary context, purpose, and objective criteria for evaluating whether any given system is "secure" as meant by these claims (if it can be discerned at all), must be fixed within the patents themselves.

Microsoft's Construction: Unlike InterTrust's proposal, Microsoft's construction of "secure" is workable, precise, and honors the basic premise of VDE. Specifically, to the extent a construction is forced onto this indefinite claim term, it should be that the term "secure" indicates

that each type of property identified in the patents is "truly secure" against all types and levels of threats identified in the patents. In part, this means that "secure" is "(1) A state in which all users of a system are guaranteed that all information, processes, and devices within the system, shall have their availability, secrecy, integrity, authenticity and nonrepudiation maintained against all of the identified threats thereto." (See JCCS Exh. A at Row 3).

This is not a standard definition of "secure." Nor is it an express definition from the Big Book (which doesn't offer one). But, if the Court denies Microsoft's indefiniteness motion, and finds the term "secure" sufficiently clear to construe, this is the fairest approach to that construction. Specifically, this "true security" construction follows from InterTrust's assertion that "security is designed to be sufficient for a particular purpose." Here, the Big Book describes a wide range of possible security threats, including strong and sophisticated attacks against valuable information where only this proposed "true security" would be acceptable. None of the patent claims excludes such high-value, strong-attack situations. On the contrary, they apparently maintain a secure state in the face of all attacks mentioned in the patents. Therefore, the fairest construction is the one that makes sense over the whole range of disclosed attack situations, namely "true security" where all properties are protected against all attacks identified in the Big Book.

X. CONSTRUCTION OF "SECURE CONTAINER"

Central Dispute: Whether a "secure container" must prevent unauthorized access to its contents.

A VDE secure container is one of the core VDE components that provide the capabilities touted in the Summary of the Invention.

Ordinary Meaning: The parties agree that the term "secure container" has no ordinary meaning in this field. (See, e.g., Reiter Depo. at 275:6-276:10.)

Microsoft's Construction: (1) A VDE Secure Container is a self-contained, self-protecting data structure which … (b) cryptographically protects that information from all unauthorized Access and Use, … (d) permits the association of itself or its contents with Controls

and control information governing (Controlling) Access to and Use thereof, and (e) prevents such Use or Access (as opposed to merely preventing decryption) until it is "opened." (See JCCS Exh. A at Row 57).

As used in the Big Book, a VDE "secure container" protects content it contains by preventing all access to and use of that content except as authorized by VDE via satisfactory execution of VDE controls associated with the secure container. In effect, a VDE secure container hides the content from users while VDE "controls" act as guards that escort authorized users to that content and supervise their use of it. (Alexander Dec. Exh. D at 20(A)-20(C), 20(E)-20(G).)

The Big Book describes details of only one embodiment of a secure container. In that embodiment, the secure container (in conjunction with the rest of VDE) blocks all direct access to its contents, and requires satisfaction of several controls, including one created by an ACCESS method[5]:

> "Even if the object is stored locally to the VDE node, **it may be stored as a secure or protected object[6] so that it is not directly accessible to a calling process. ACCESS method 2000 establishes the connections, routings, and security requisites needed to access the object.**" ('193 192:14-19)

A secure container, then, is part of the second layer of protection discussed above. As noted in the below quote, not only is the content "encrypted" (first layer of protection) but so is the "content source and routing information" (second layer).

> "ACCESS method 2000 reads the ACCESS method MDE from the secure database, reads it in accordance with the ACCESS method DTD, and **loads encrypted content source and routing information** based on the MDE (blocks 2010, 2012). **This source and routing information specifies the location of the encrypted content.** ACCESS method 2000 then determines whether a connection to the content is available (decision block 2014). ('193 192:36-52)

---

[5] InterTrust construes "access" as meaning "To obtain something so it can be used," which is true, although incomplete.

[6] This sentence refers to a "secure object." In VDE, a "container" and its contents "can be called an 'object.'" ('193 58:43-44).

Prof. Maier explains this VDE "secure container" mechanism at greater length. (See also Reiter Depo. at 117:18-23; 125:20-126:4; '683 Patent 15:67-16:4. Maier Decl. at 38-41.)

This "access control" ability of VDE secure containers is critical to VDE's promise to content owners that it can prevent (not simply detect) all access to and use (not just decryption-based uses) of protected content. Without this access control ability of VDE generally, and secure containers in particular, VDE's promised ability to control, govern, audit, etc. all accesses and uses, would be a lie.

InterTrust's Proposed Construction: InterTrust's proposed construction of "secure container" is a far cry from the VDE "secure container": "A Container that is Secure." (See JCCS Exh. A at Row 57). As this is interpreted by Prof. Reiter, merely detecting a single form of misuse of some of its contents, would make a container a "secure container," even if the container could not prevent **any** unwanted access, misuse or interference with the contents. That certainly does not sound "secure," and, more importantly, makes no sense in light of the Big Book's and other InterTrust patents' proclamations of the abilities of a VDE secure container:

> "**Use of secure electronic containers to transport items provides an unprecedented degree of security, trustedness and flexibility.**" ('683 8:50-52).
>
> "Even if the object is stored locally to the VDE node, **it may be stored as a secure or protected object so that it is not directly accessible to a calling process. ACCESS method 2000 establishes the connections, routings, and security requisites needed to access the object.** ('193 188:59-67).

XI. CONSTRUCTION OF "TAMPER RESISTANT BARRIER"

Central Dispute: Whether a "tamper resistant barrier" must be a physical device, and prevent unauthorized access, observation, and interference.

Another of the required VDE mechanisms for providing the promised VDE capabilities, is a VDE secure processing environment, formed by a hardware-based tamper resistant barrier.

Ordinary Meaning: The ordinary meaning of "tamper resistant barrier" denotes a physical device. More specifically, the term "tamper resistant barrier" would have been understood in 1995 in reference to cryptographic coprocessors such as smart cards. (See Reiter Depo. at 137:15 – 138:17).

Microsoft Construction: "(1) An active device that encapsulates and separates a Protected Processing Environment from the rest of the world. (2) It prevents information and processes within the Protected Processing Environment from being observed, interfered with, and leaving except under appropriate conditions ensuring security. (3) It also Controls external access to the encapsulated Secure resources, processes and information. (4) A Tamper Resistant Barrier is capable of destroying protected information in response to Tampering attempts." (See JCCS Exh. A at Row 71).

To properly construe this term requires consideration of another "access control" promise of VDE.

As noted above, VDE concerns both security **and** commerce. Hence, it does not just prevent unauthorized access to protected content, it also allows and governs authorized access to, and use of, that content. That, however, presents a possible security hole. The processes used to allow and govern authorized access or use might be observed by attackers and altered to permit improper access to and use of protected content. Therefore, as a corollary to its promise to prevent protected **content** from any unauthorized access, VDE also promises that it is capable of preventing (not merely detecting) all unauthorized observation of and interference with the VDE **processes** which govern such access and use.[7]

> "SPU 500 is enclosed within and protected by a '**tamper resistant security barrier' 502. Security barrier 502 separates the secure environment 503 from the rest of the world. It prevents information and processes within the secure environment 503 from being observed, interfered with and leaving except under appropriate secure conditions.**" ('193 59:48-53)

> "SPU 500 provides a tamper-resistant protected processing environment ("PPE") in which processes and transactions can take place securely and in a trusted fashion." ('683 16:60-62)

Prof. Reiter has agreed that the Big Book describes mechanisms to prevent all types of tampering (unauthorized interference) with VDE processes. (Reiter Depo. at 55:17-60:1).

---

[7] Whether users can choose not to use all of a system's capabilities does not change the fact that those capabilities allegedly exist.

This corollary promise—the ability to prevent VDE processes from unauthorized observation and interference—informs the proper construction of "tamper resistant barrier." As described in the first above quote, a tamper resistant barrier encapsulates a special-purpose "Secure Processing Unit" (SPU). This physical tamper resistant barrier prevents both information and processes within the Protected Processing Environment from being "observed, interfered with, and leaving" except under appropriate conditions ensuring security.

> "SPU 500 in this example is an integrated circuit ("IC") "chip" 504 including "hardware" 506 and "firmware" 508. ... "Hardware" 506 also contains long-term and short-term memories to store information securely so **it can't be tampered with.**" ('193 59:60-60:3)

> "BIU 530 is **designed to prevent unauthorized access to internal components within SPU 500 and their contents.** It does this by only allowing signals associated with an SPU 500 to be processed by control programs running on microprocessor 520 and not supporting direct access to the internal elements of an SPU 500." ('193 69:6-11)

As InterTrust notes, the Big Book also refers to a "tamper resistant barrier" which is not a physical, hardware device. However, the "tamper resistant barrier" in the mini-Markman claims is properly construed as the hardware variant, for three reasons.

First, the Big Book promises "true" security. It promises the ability to "prevent" unauthorized uses, etc., and "ensure" that rights will be enforced, and "guarantee" trustworthiness, even when faced with strong, sophisticated attacks against high-value content. Nothing in the claims indicates an inability to live up to these promises and protect such high-value content against such strong attacks. Only the hardware-based tamper resistant barrier is described as providing that sort of true protection for the most valuable content in even high-risk surroundings.

> "HPEs 655 may (as shown in FIG. 10) be provided with a software- based tamper resistant barrier 674 that makes them more secure. Such a software-based tamper resistant barrier 674 may be created by software executing on general-purpose CPU 654. Such a 'secure' HPE 655 can be used by ROS 602 to execute processes that, while still needing security, may not require the degree of security provided by SPU 500. This can be especially beneficial in architectures providing both an SPE 503 and an HPE 655. **The SPU 502 may be used to perform all truly secure processing, whereas one or more HPEs 655 may be used to provide additional secure (albeit possibly less secure than the SPE) processing** using host processor or other general purpose resources that may be available within an

electronic appliance 600. Any service may be provided by such a secure HPE 655" ('193 80:22-36)

> "**No software-only tamper resistant barrier 674 can be wholly effective against all of these threats. A sufficiently powerful dynamic analysis (such as one employing an in-circuit emulator) can lay bare all of the software-based PPE 650's secrets.** Nonetheless, various techniques described below in connection with FIG. 69A and following make such an analysis extremely frustrating and time consuming--increasing the 'work factor' to a point where it may become commercially unfeasible to attempt to 'crack' a software-based tamper resistant barrier 674." ('900 233:24-33)

Second, if these claim terms were construed to cover the software variants, they would be much too vague. There would be no objective measure for distinguishing between a barrier which is tamper resistant and one which is not tamper resistant.

Third, the Big Book states that a Secure Processing Unit (with its physical tamper resistant barrier) is **necessary** wherever protected content is assigned usage related control information, or used. As all of the mini-Markman claims contemplate one or both of these two conditions, each claim necessarily requires a hardware tamper resistant barrier.

> "VDE allows the needs of electronic commerce participants to be served and it can bind such participants together in a universe wide, trusted commercial network that can be secure enough to support very large amounts of commerce. **VDE's security and metering secure subsystem core will be present at all physical locations where VDE related content is (a) assigned usage related control information (rules and mediating data), and/or (b) used. This core can perform security and auditing functions (including metering) that operate within a 'virtual black box,' a collection of distributed, very secure VDE related hardware instances** that are interconnected by secured information exchange (for example, telecommunication) processes and distributed database means." ('193 15:14-27)

> "**Summary of Some Important Features Provided by VDE in Accordance With the Present Invention** ... VDE employs **special purpose hardware** distributed throughout **some or all locations** of a VDE implementation: a) **said hardware controlling important elements of**: content preparation (such as causing such content to be placed in a VDE content container and associating content control information with said content), content **and/or** electronic appliance usage auditing, content usage analysis, **as well as content usage control**; and b) said hardware having been designed to securely handle processing load module control activities, wherein said control processing activities may involve a sequence of required control factors" ('193 21:43-45; 22:20-31)

> "**A hardware SPU (rather than a software emulation) within a VDE node is necessary if a highly trusted environment for performing certain VDE activities is required.**" ('193 49:15-17)

> "**Physical facility and user identity authentication security procedures** may be used **instead of hardware SPUs** at **certain nodes**, such as at an established financial clearinghouse, **where such procedures may provide sufficient security** for trusted interoperability with a VDE arrangement employing hardware SPUs at user nodes." ('193 45:60-65)

(See also Maier Decl. at 9-11.)

InterTrust's Proposed Construction: "Hardware and/or software that provides Tamper Resistance." InterTrust defines "Tamper Resistance" as "Making tampering more difficult and/or allowing detection of tampering." (See JCCS Exh. A at Row 67).

This proposal raises more questions than it answers. For example, "making tampering more difficult" than what? What does "allowing detection of tampering" mean? Not preventing detection? Are the walls of straw house a tamper resistant barrier because they allow detection of a fire? And, as usual, InterTrust's proposed construction is contrary to VDE. The "invention" did not settle for mere detection; it was touted as preventing all unauthorized access, use, observation, and interference. InterTrust may regret those promises but it cannot erase them.

XII. CONSTRUCTION OF "PROTECTED PROCESSING ENVIRONMENT"

Central Dispute: Whether a "protected processing environment" must have a physical "tamper resistant barrier" and prevent unauthorized access, observation, and interference.

This claim term presents the same key issue as "tamper resistant barrier."

Ordinary Meaning: The parties agree that there is no ordinary meaning of "protected processing environment."

Microsoft Construction: "(1) A uniquely identifiable, self-contained computing base trusted by all VDE nodes to protect the availability, secrecy, integrity and authenticity of all information identified in the February, 1995, patent application as being protected, and to guarantee that such information will be Accessed and Used only as expressly authorized by VDE Controls. (2) At most VDE nodes, the Protected Processing Environment is a Secure Processing Environment . . . (3) The Tamper Resistant Barrier prevents all unauthorized (intentional or accidental) interference, removal, observation, and use of the information and processes within it,

by all parties (including all users of the device in which the Protected Processing Environment resides), except as expressly authorized by VDE Controls." (See JCCS Exh. A at Row 62).

As InterTrust notes, the Big Book describes two categories of processing environment. One, called a Secure Processing Environment (SPE), is hardware-based, centered on the Secure Processing Unit (SPU) with a hardware tamper resistant barrier. This SPE is said to provide "true" security. Another, called a Host Processing Environment (HPE), lacks an SPU, and if it has any tamper resistant barrier, it is software based. The Big Book says that an HPE provides less protection and may not be "truly secure." The patent uses the term "Protected Processing Environment" to refer to either an SPE, or HPE, except as otherwise indicated. And, it says that an HPE may be "secure" or "non-secure." (Alexander Dec. Exh. D at 16(C), 16(H), 16(I), 18(A)-18(E).)

The same three reasons cited above for "tamper resistant barrier" also demonstrate that these claims' "protected processing environment" must be the hardware-based Secure Processing Environment, not the software-based Host Processing Environment.

InterTrust's Proposed Construction: (1): "An environment in which processing and/or data is at least in part protected from tampering. The level of protection can vary, depending on the threat . . . ." (See JCCS Exh. A at Row 62).

This definition is vague in several respects. For example, what does it mean to "at least in part protect" processing and/or data? What exactly does the "in part" modify? Does protection mean prevention, or is merely allowing detection good enough as InterTrust suggests for "secure"? And, as the level of protection depends on the threat, what precise threat(s) are assumed by this claim term, and what "level of protection" is required by those threats? And, is the "processing and/or data" inside the environment being protected from the outside world, or is the outside world being protected from what's inside the environment? In any event, InterTrust's proposal again fails to honor any of the requirements of the VDE "invention," including its ability to prevent all unauthorized access, use, observation, and interference.

XIII. CONSTRUCTION OF "COMPONENT ASSEMBLY"

Central Dispute: Whether a "component assembly" is executable.

In the disclosed "invention," "component assemblies" are dynamically created executable components (called VDE's "basic functional unit") which help give VDE its touted flexibility and user-configurability.

Ordinary Meaning: The parties agree that the term "component assembly" has no ordinary meaning in this art.

Microsoft's Construction: "(1) A cohesive Executable component created by a channel which binds or links together two or more independently deliverable Load Modules ..., and associated data; ...." (See JCCS Exh. A at Row 99).

In the Big Book, the term "component assembly" (also called "component") uniformly is used to refer to executable components, which are an assembly of independent, executable load modules and data. These VDE component assemblies may be transferred between VDE nodes to perform various tasks, and each is "executable." (See Alexander Dec. Exh. D at 24-4(CC), 6(B, C).) The **only** kind of "component assembly" mentioned in these patents is this VDE component assembly.

InterTrust's Proposed Construction: "Components are code and/or data elements that are independently deliverable...." There is no support for this notion that a component assembly may be mere non-executable data. None of the above-quotes (e.g., "component assemblies 690 are the basic functional unit") would make any sense if the component assembly were not executable. Indeed, as noted below, the most important executable component in VDE—the VDE control—is a component assembly.

XIV. CONSTRUCTION OF "CONTROL" (NOUN)

Central Dispute: Whether a "control" is an executable component.

Satisfactory execution of "VDE controls" give authorized users access to content protected by VDE secure containers and VDE protected processing environments.

Ordinary Meaning: While the term "control" is used frequently in computer science, it does not have any precise ordinary meaning, but rather means different things in different contexts.

Microsoft's Construction: "(1) Independent, special-purpose, Executable, which can execute only within a Secure Processing Environment. (2) Each VDE Control is a Component Assembly dedicated to a particular activity (e.g., editing, modifying another Control, a user-defined action, etc.), particular user(s), and particular protected information, and whose satisfactory execution is necessary to Allowing … that activity…." (See JCCS Exh. A at Row 4).

VDE "controls" can be explained, partially, with an analogy to a rare books library holding valuable texts. Each different type of access and use of these texts is controlled by a different set of rules, and possibly a different guard or librarian. One guard checks one list of permitted visitors to enter the library; another may check a shorter list for entry to a particular room with particularly valuable texts; another librarian will follow other rules to collect certain texts and supervise their viewing; another may follow other rules to determine whether the visitor may copy any portion of the text; and another may need to authorize or stay after hours to translate (decrypt) the text, or perhaps only particular pages thereof. In VDE, these separate guards and librarians are independent, executable VDE controls which, based on applicable rules, allow a particular type of access or use, and then monitor that access or use. Prof. Maier's explanation of VDE explains an example of these independent VDE controls in operation.

The Big Book states that an important feature of VDE is that each VDE control specializes in allowing and supervising only one type of access or use. VDE controls independently govern separate activities (e.g., access or copy or read); independently govern arbitrarily small portions of data; and are configurable by all participants (subject only to other participants' controls).

> "**Secure electronic controls** can specify how an item is to be processed or otherwise handled (e.g., document can't be modified, can be distributed only to specified persons, collections of persons, organizations, can be edited only by certain persons and/or in certain manners, can only be viewed and will be 'destroyed' after a certain elapse of time or real time or after a certain number of

> handlings, etc.) **Persistent secure electronic controls** can continue to supervise item workflow even after it has been received and 'read.'" ('683 6:18 - 9:4)

InterTrust's Proposed Construction: InterTrust's proposed construction of "Control" again ignores the Big Book in favor of a vague, non-VDE construction: "Information and/or programming Governing operations on or use of Resources (e.g., content) including (a) permitted, required or prevented operations, (b) the nature or extent of such operations or (c) the consequences of such operations." (See JCCS Exh. A at Row 4). With its "information and/or programming" language, InterTrust suggests that a "control" may be mere non-executable information. More specifically, InterTrust has equated non-executable "rules" and executable "controls." This confuses the guard (control) with the rules he or she follows in allowing and monitoring certain accesses or uses. In the Big Book's usage, a "rule" need not be executable, but a "control" must be.

InterTrust argues that "rules and controls" are equated with "control information," and control information may be mere data, and therefore a control may be mere data. But, under that "logic," apples may be oranges because a sentence in a text reads "apples and oranges (fruit)." The patents do not equate rules and controls, but rather distinguish them by, e.g., often referring to "rule **and/or** control":

> "...at least one **rule and/or control** associated with the software agent that governs the agent's operation." ('193 241:2-3)

> "If necessary, trusted go-between 4700 may obtain and register any methods, **rules and/or controls** it needs to use or manipulate the object 300 and/or its contents (FIG. 122 block 4778)." ('683 47:42-45)

Just as it makes no sense to refer to "apple and/or apple," it would make no sense to refer to "rule and/or control" if they were the same.

XV. <u>CONSTRUCTION OF SOME OTHER TERMS AND PHRASES</u>

<u>"A budget specifying the number of copies which can be made of said digital file"</u> (JCCS Exh. A at Row 6): InterTrust's proposed construction refers to a budget "stating the number of copies that can be made of the digital file," without specifying "can be made since when?" or "by

whom?" or "by what?" Microsoft's construction answers these open questions. (See also Reiter Depo. at 267:18-268:15.)

"Container" (JCCS Exh. A at Row 57): InterTrust proposes that a "container" "means a digital file containing linked and/or embedded items." Prof. Reiter, however, could think of no non-empty digital file which did not "contain linked and/or embedded items," and thus all digital files would qualify as "containers." That is not how this term is used in InterTrust's patents. (See Alexander Decl. Exh. D at 20(A-D).)

"Containing" (JCCS Exh. A at Row 58): The parties disagree on whether storing an indication of where an element may be found, constitutes "containing" that element. The patents are internally inconsistent on this; sometimes saying that "referencing" something is "containing" it; and other times indicating that "referencing" something is an alternative to "containing" it. (See, e.g., Alexander Decl. Exh. D at 24-8(I) ("containing or referencing").) As the normal, ordinary meaning of "contain" is to include within, not reference, the Court should adopt that meaning.

"Controlling" (JCCS Exh. A at Row 7): InterTrust's proposed construction of "control" as a verb is typically vague: "to exercise authoritative or dominating influence over; direct." This loose "influence" of the sort pertinent to persons, not computers, is not what the Big Book promises the owners of content entrusted to VDE. They were promised strict control (including monitoring) over all access and uses, including the ability to prevent (not merely detect) unauthorized access and use. (See Reiter Depo. at 165:3-9.)

Moreover, "controlling" in this "invention" is done at an arbitrary granularity, which is an important feature that the Big Book relied upon to distinguish prior art:

> **"VDE also** extends usage control information to an arbitrary granular level **(as opposed to a file based level provided by traditional operating systems)"**

(See Alexander Decl. Exh. D at 24-4(X) ('193 275:8-11)).

"Controlling the copies made of said digital file" (JCCS Exh. A at Row 7): Whereas the claim refers to "controlling the copies," InterTrust reads the claim more as "controlling the

copying." Also, InterTrust's proposal suggests that the copies are transferred to the second device, but the claims recite that the file (as opposed to any copy) is transferred.

"Derives information from one or more aspects of said host processing environment" (JCCS Exh. A at Row 92): Prof. Reiter links this claim language to the "machine signature" technique described in the '900 Patent. That technique derives a "unique" signature of an appliance so that the HPE-forming software will not run on any other appliance. InterTrust's proposed construction lacks this "unique machine signature" technique. Under InterTrust's proposed construction, the derived information may serve no security purpose at all, which again is contrary to the patent.

"Host Processing Environment" (JCCS Exh. A at Row 87): The Big Book states that a "Host Processing Environment" may be secure or not secure. InterTrust's proposed construction requires security, and thus is contrary to the Big Book. Microsoft's construction explains what it means in the Big Book for a "host processing environment" to be non-secure.

"Identifying (Identify)" (JCCS Exh. A at Row 28): In common usage and these patents, to identify someone or something is to establish the person or thing as a particular individual or thing. InterTrust tries to expand this common understanding with its proposal: "establishing the identity of or to ascertain the origin, nature, or definitive characteristics of; ...." This is contrary to the ordinary meaning, and, again, too vague. Is gray hair a "definitive characteristic" of a person? Is a particular manufacturer of a device sufficient to establish its "nature?" The jury and public would have to guess.

"Tamper Resistance" (JCCS Exh. A at Row 67): InterTrust's proposed construction, "Making tampering more difficult and/or allowing detection of tampering," suffers from the same type of defects as InterTrust's other proposals. For example, "more than difficult than what?" Also, merely detecting tampering but not stopping it, plainly is not what VDE means by "tamper resistance."

For the foregoing reasons, Microsoft's proposed constructions should be adopted.

Dated: April 7, 2003

By: ________________
ERIC L. WESENBERG

KEKER & VAN NEST, LLP
JOHN W. KEKER - #49092
MICHAEL H. PAGE - #154913
710 Sansome Street
San Francisco, CA 94111-1704
Telephone: (415) 391-5400
Facsimile: (415) 397-7188

DERWIN & SIEGEL, LLP
DOUGLAS K. DERWIN - #111407
3280 Alpine Road
Portola Valley, CA 94028
Telephone: (408) 855-8700
Facsimile: (408) 529-8799

INTERTRUST TECHNOLOGIES CORPORATION
JEFFERY J. McDOW - #184727
4800 Patrick Henry Drive
Santa Clara, CA 95054
Telephone: (408) 855-0100
Facsimile: (408) 855-0144

Attorneys for Plaintiff and Counter-Defendant
INTERTRUST TECHNOLOGIES CORPORATION

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

INTERTRUST TECHNOLOGIES CORPORATION, a Delaware corporation, Plaintiff, v. MICROSOFT CORPORATION, a Washington corporation, Defendant.	Case No. C 01-1640 SBA (MEJ) Consolidated with C 02-0647 SBA **PLAINTIFF INTERTRUST TECHNOLOGIES CORPORATION'S REPLY MEMORANDUM ON CLAIM CONSTRUCTION** Date: May 12, 29, & 30, 2003 Time: 9:00 a.m.
AND COUNTER ACTION.	

TABLE OF CONTENTS

TABLE OF CONTENTS
(cont'd)

TABLE OF AUTHORITIES

TABLE OF AUTHORITIES
(cont'd)

Page(s)

Other Authorities

I. INTRODUCTION

Microsoft's claim construction positions derive from a single underlying premise: the details of the "VDE" embodiment described in the specifications must be read into every claim, and every claim element must be interpreted so as to include all of the VDE limitations. According to Microsoft, this is so because the patents "promise" an extremely high degree of security ("truly secure") that Microsoft alleges can only be supplied by the VDE embodiment.

Microsoft acknowledges, however, that the patents describe varying levels of security, ranging from the extremely high degree of security provided by the "truly secure" embodiment to much lower levels of security. The patents refer to all of these levels of security as "secure," and each of them represents a degree of security appropriate to particular circumstances. Microsoft's constructions exclude all levels of security other than the extremely high "truly secure," not because the claims specify this high level of security (they are silent regarding the particular level of security required and do not mention "true" security), not because the specification requires such an interpretation (it describes varying degrees of security) and not because the ordinary meaning of the claim terms requires such an interpretation (Microsoft acknowledges its definition of "secure" is not standard).

Instead, Microsoft excludes all levels of security other than the highest possible level because, according to Microsoft, only the highest possible level is consistent with the "VDE invention." Microsoft contends that lower security embodiments should be ignored during claim construction, because in some places the specification uses the word "invention" in combination with VDE, thereby allegedly requiring that 115 pages, including "literally hundreds" of limitations, be read into every claim.

Microsoft's requirement that the "VDE invention" be imported into every claim leads Microsoft to claim constructions that directly contradict the definition given to the same terms in the specification. For example, the specification describes two embodiments of "tamper resistant barrier," a higher-security hardware embodiment and a lower-security software embodiment. Both of these embodiments are identified in the specification as a "tamper resistant barrier." Microsoft, however, demands that the claim term "tamper resistant barrier" be defined to exclude

the software embodiment, since the software embodiment is inconsistent with Microsoft's requirement that VDE "true security" be read into every claim. Similarly, the specification describes two embodiments of "protected processing environment," a higher-security hardware embodiment and a lower-security software embodiment, both identified in the specification as a "protected processing environment." Microsoft's construction of "protected processing environment" excludes the software embodiment, again because this is inconsistent with Microsoft's requirement that VDE "true security" be read into every claim element.

The Federal Circuit has held that claim constructions that exclude disclosed embodiments are "rarely, if ever" correct. Microsoft's "VDE invention" construction of the claims ignores specification embodiments describing levels of security different than extremely secure "true" security, and contradicts the specification's use of the claim terms. Microsoft's construction must therefore be rejected as being inconsistent with the patent specifications.

II. ARGUMENT

A. Microsoft's Requirement of Absolute, "True" Security Contradicts the Specification.

1. Microsoft's VDE construction requires that the claims be interpreted to require an extremely high degree of security.

Microsoft's proposed constructions require that "each type of property identified in the patents is 'truly secure' against all types and levels of threats identified in the patents." MS Br., 28:1-2. According to Microsoft, this requires that "all users" are "guaranteed that all information, processes, and devices" will have five separate properties "maintained against all of the identified threats thereto." MS Br., 28:2-5. Microsoft justifies this extreme position by arguing that none of the patents excludes what Microsoft characterizes as "true security." MS Br., 28:7-17. Thus, Microsoft's brief includes statements such as the following:

> [T]he Big Book promises **"true" security**. It promises the ability to "prevent" unauthorized uses, etc., and "ensure" that rights will be enforced, and "guarantee" trustworthiness, even when faced with strong, sophisticated attacks against high-value content. Nothing in the claims indicates an inability to live up to these promises and protect such high-value content against such strong attacks.

MS Br., 32:16-20 (emphasis added). See also Id., 3:4-11, 17:4-6.

Microsoft asks that claims be interpreted narrowly so as to exclude all levels of security other than this "true" security, security so high as to amount to an absolute "guarantee" of protection against all threats, "no matter what effort may be made" to break the protection.

2. The specification discloses embodiments that do not require the highest degree of security.

As Microsoft acknowledges, the patents describe a variety of levels of security. Thus, Microsoft states that the patents use "secure" "to mean different things in different places," (MS Br., 25:18-19), and "the term 'secure' is used in the specification to refer to different things in different contexts." MS Br., 27:10-11.

The passage Microsoft relies upon for its requirement of "true" security makes exactly this point:

> The SPU 502 may be used to perform all **truly secure** processing, whereas one or more HPEs 655 may be used to provide **additional secure (albeit possibly less secure** than the SPE) processing . . . **Any service may be provided by such a secure HPE** . . . .

'193 patent, 80:30-36 (JCCS Ex. C, 22(B) (emphasis added).

Other passages similarly indicate that different degrees of protection may be desirable in different contexts:

> Because security may be better/more effectively enforced with the assistance of hardware security features such as those provided by SPU 500 (and because of other factors such as increased performance provided by special purpose circuitry within SPU 500), **at least one SPE 503 is preferred for many or most higher security applications. However, in applications where lesser security can be tolerated** and/or the cost of an SPU 500 cannot be tolerated, **the SPE 503 may be omitted and all secure processing may instead be performed by one or more secure HPEs** 655 executing on general-purpose CPUs 654.

'193 patent at 80:65-81:8 (JCCS Ex. C, 19(N)) (emphasis added). Additional examples of specification passages describing security levels below the highest level are found at JCCS Ex. C, 19(B), (C), (J), and (M).

Thus, the parties agree that the patent specification describes different degrees of security, including "truly" secure and "less" secure. The word "secure" is used to refer to both of these levels.

3. The patent claims do not specify a high degree of security.

The claims do not require "true" security. Both disclosed embodiments (truly secure and less secure) are within the scope of the word "secure" as used in the specification.

That "secure" is used to refer to different levels and degrees of security supports InterTrust's definition, since that definition allows such different degrees. Microsoft, however, argues that the breadth given to the term in the specification actually supports reading the most extreme disclosed embodiment into the claims, on the theory that the claims do not "exclude" this embodiment. MS Br., 28:12-13.[1] Microsoft further alleges that the context of the claims requires "true security" against "high-value, strong attack situations." MS Br., 28:9-17.

Microsoft fails, however, to adequately explain how the "context" of any particular claim requires the highest degree of security described in the patent specification. Claim 193.1, for example, involves downloading and playing music. This hardly seems the type of "high value, strong-attack" situation Microsoft describes. Microsoft gives no reason for assuming that the value and potential threats applicable to downloading songs is the same as the value and threats relevant, for example, to corporate trade secrets, nuclear weapons codes, money wire transfers, etc.

4. Microsoft's massive definition of "secure" invites the Court to usurp the jury's role in conducting the infringement analysis.

"Secure" is a general term, and the degree of protection necessary for a system to be "secure" depends on the context. The parties are in agreement on this, as is the specification.

When a claim term is drafted in general terms that may cover a range of circumstances, the Federal Circuit mandates that the Court construe the term generally and leave the question of determining whether an accused product meets that general construction to the finder of fact:

> Claims are often drafted using terminology that is not as precise or specific as it might be. . . . That does not mean, however, that a court, under the rubric of claim construction, may give a claim whatever additional precision or specificity is necessary to facilitate a comparison between the claim and the accused product. Rather, after the court has defined the claim with whatever specificity and precision is warranted by the language of the claim and the evidence bearing on the proper construction, the task of determining whether the construed claim reads

[1] InterTrust agrees that the claims do not exclude the "true security" embodiment. That claims do not exclude an embodiment obviously does not mean the claims require that embodiment.

on the accused product is for the finder of fact.

> The proper allocation of the tasks of construing a claim and determining infringement in a case in which a claim contains an imprecise limitation is demonstrated by our decision in Modine Mfg. Co. v. United States Int'l Trade Comm., 75 F.3d 1545, 37 U.S.P.Q.2D (BNA) 1609 (Fed. Cir. 1996). In Modine, the patentee had claimed a condenser for an automotive air conditioning system with "relatively small" hydraulic diameters. Id. at 1549. From the specification and prosecution history of the patent, this court concluded that the term "relatively small" should be interpreted as referring to a range of diameters of "about 0.015-0.040" inches. Id. at 1554. Instead of attempting to define that range more precisely, we remanded the case for a factual determination of whether the claim limitation was literally infringed by accused products having diameters ranging from 0.0424 to 0.0682 inch. Id. at 1554-55.
>
> [T]he '886 patent contains some inherent imprecision resulting from the use of the term "consisting essentially of." As PPG points out, it is possible that under such circumstances different finders of fact could reach different conclusions regarding whether the effect of a particular unlisted ingredient in an accused product is material, and thus whether that product infringes. That possibility, however, is a necessary consequence of treating infringement as a question of fact subject to deferential review. It does not mean that the claim was improperly construed as an initial matter.

PPG Indus., Inc. v. Guardian Indus. Corp., 156 F.3d 1351, 1355 (Fed. Cir. 1998) (citation omitted).

PPG Industries is controlling here. "Secure" is a general term, the applicability of which depends on the context. The parties agree on this, and the patents describe different levels of security. The Court should, therefore, construe the term generally, and allow the jury to determine whether, under the particular circumstances, an accused product is or is not "secure."

B. Microsoft's VDE-Based Interpretation Requires Excluding Disclosed Embodiments.

The Federal Circuit is clear on constructions that exclude disclosed embodiments:

> A claim construction that does not encompass a disclosed embodiment is thus "rarely, if ever, correct and would require highly persuasive evidentiary support." Vitronics, 90 F.3d at 1583, 39 U.S.P.Q.2D (BNA) at 1578.

Johns Hopkins Univ. v. CellPro, Inc., 152 F.3d 1342, 1355 (Fed. Cir. 1998) (emphasis added).

Microsoft's VDE-based constructions lead to exactly this result.

1. Tamper-Resistant Barrier.

Microsoft argues that "tamper resistant barrier" must be interpreted as a hardware device. MS Br., 30:22-23. As Microsoft acknowledges, however, "the Big Book also refers to a 'tamper

resistant barrier' which is not a physical hardware device." MS Br., 32:13-14.[2] In fact, the patent discusses this software embodiment at length, using the phrase "tamper resistant barrier" to refer to it. JCCS Ex. C, 22(B). Microsoft would thus have the Court construe "tamper resistant barrier" to exclude an embodiment identified in the specification as a "tamper resistant barrier." Why? Because defining "tamper resistant barrier" to include the software embodiment is inconsistent with VDE requirements Microsoft seeks to read into all of the claims (e.g., "true security," hardware Secure Processing Unit"). MS Br., 32:13-34:4.[3]

Microsoft's VDE construction is inconsistent with interpreting "tamper resistant barrier" to include the software "tamper resistant barrier." The Court therefore has a choice: accept Microsoft's VDE argument and construe this term in a manner contradicting the specification, or reject Microsoft's VDE construction and construe the term as it is used in the specification. As the Federal Circuit has held, the former of these approaches is "rarely, if ever" correct.

Moreover, InterTrust is aware of no Federal Circuit case that has ever held that a claim term can be interpreted to exclude, not merely a disclosed embodiment, but a disclosed embodiment that is identified in the specification <u>using exactly the same words as the claim</u> ("tamper resistant barrier"). Yet this is the result mandated by Microsoft's VDE construction.[4]

2. Protected processing environment.

Microsoft acknowledges that the specification discloses two embodiments of a protected processing environment, a hardware-based SPE and a software-based HPE, both of which are

---

[2] Microsoft also alleges that the "ordinary meaning" of tamper resistant barrier connotes a physical device (MS Br., 30:24-28), but neither of its experts testifies to this effect, and Microsoft's only support is a misleading citation to Dr. Reiter, testimony that Dr. Reiter explicitly characterized as "an example." Reiter I, 137:22. (Keefe Decl., Ex. E.)

[3] Microsoft also alleges in a conclusory manner that a software tamper resistant barrier would be too vague since "there would be no objective measure for distinguishing between a barrier which is tamper resistant and one which is not tamper resistant" (MS Br., 32:7-9), but fails to discuss the lengthy specification disclosure discussing the software tamper resistant barrier (JCCS Ex. C, 22(B)), nor does Microsoft address why a tamper resistant barrier provided by software requires an "objective measure" whereas no such objective measure is required for a hardware barrier.

[4] Moreover, the claim itself is inconsistent with Microsoft's interpretation. 721.1 recites not one but two tamper resistant barriers, and further recites that they have different security levels. The claim therefore clearly contemplates the possibility that one tamper resistant barrier will be more secure than another. For example, in one obvious embodiment, the first tamper resistant barrier would be hardware (higher security) and the second would be software (lower security).

explicitly identified as "protected processing environments." MS Br., 34:3-14. As Microsoft further acknowledges, Microsoft's definition of "protected processing environment" excludes the software-based HPE embodiment. MS Br., 35:3-14.

According to Microsoft, this is mandated for the same reason as exclusion of the software "tamper resistant barrier" from the construction of that term. MS Br., 35:12-14. Again, Microsoft's VDE-based construction requires excluding a disclosed embodiment from the definition of a claim term, even though that embodiment is <u>explicitly identified in the specification</u> using the exact same term, and even though the specification explicitly states that "any service" may be provided by a secure HPE. '193 Patent, 80:35-36 (JCCS Ex. C, 22(B)).

Interpretation of claim terms so as to exclude embodiments distinctly described in the specification is clear legal error, yet this is precisely the result of Microsoft's VDE-centric position.

C. Microsoft's Legal Arguments Are Misleading.

Microsoft's General Claim Construction Legal Analysis cites sources for the proposition that claims must recite the invention described in the specification. MS Br., 9:14-26. Microsoft emphasizes the word "invention" in these quotations, apparently hoping the Court will conclude that these cases and statutes stand for the proposition that, when the specification uses the word "invention," every element described thereafter must be read into every claim.

In fact, none of the cited authority supports this proposition. That claims must recite the invention described in the specification does not mean that when a patent specification uses the word "invention," the specification is automatically imported into the claims. InterTrust cited numerous Federal Circuit cases in its opening brief holding that elements described as the "invention" should not be read into the claims. InterTrust's Opening Br., 9:1-10:24. Microsoft does not even attempt to distinguish this authority.

D. Microsoft's Argument that the Claims Require VDE is Wrong.

1. '193 patent claims.

The '193 patent's claims do not refer to "VDE," nor to any other coined terms, such as "protected processing environment" or "host processing environment." In its attempt to

shoehorn VDE into these claims, despite the absence of any VDE language, Microsoft relies on a variety of arguments that it repeats with respect to the other claims. First, Microsoft argues that the claims require elements that are not present in the claims themselves:

> All four '193 Patent mini-Markman claims concern the distribution and protection of digital content, and contemplate multiple nodes and participants. Information is received (**possibly** from multiple upstream content providers), then stored on a device having **unspecified** authorized and unauthorized users, and then conditionally transferred to another device having **unspecified** users.

MS Br., 16:22-26 (emphasis added).

Why are the multiple content providers and multiple users "possible" and "unspecified?" <u>Because the claims do not require them</u>. The claims do not refer to multiple upstream content providers. The claims do not refer to multiple users of the first device, much less authorized and unauthorized users. The claims do not refer to multiple users of the second device.

The InterTrust claims are silent on these questions. The claims are <u>consistent with</u> multiple upstream content providers, but do not <u>require</u> them. The claims are <u>consistent with</u> multiple users of the first device, but do not <u>require</u> them. The claims are <u>consistent with</u> multiple users of the second device, but do not <u>require</u> them.

That claims are consistent with a particular embodiment is hardly grounds for reading every limitation from that embodiment into the claims.

Prof. Maier's Declaration includes testimony that is apparently intended to buttress Microsoft's argument. That testimony is worth quoting in full:

> Additional **compelling evidence** of the presence of the Virtual Distribution Environment can be found in the process described in the claims themselves. For example, '193 Patent claim 1 purports to describes a distribution process involving at least three nodes. Thus, "receiving a digital file" implies, although does not explicitly state, that the digital file must come from some source device or system regardless of the transmission mechanism. Logically, this would be a system other than the "first device" and the "second device" which are described in other steps of the claim. Otherwise, the claim would have questionable utility.

Maier Decl., 23:17-25 (emphasis added).

This is typical of Microsoft's Markman positions in general. Prof. Maier establishes that a "received" digital file must come from somewhere (a point not disputed by InterTrust), but

fails to explain why this is "compelling evidence" that the claims require VDE. Calling something "compelling evidence" does not make it so.

Microsoft's argument proceeds as follows:

> This claim language (e.g., "if . . . allows," "determining whether") is not qualified. It implies that if the copying and storing are not allowed, then they are prevented (see Reiter Depo. at 174:1-178:11), no matter what effort may be made to take the unauthorized action. In other words, these claims imply that their "controls" are effective in the face of the attacks identified in the Big Book.
>
> These claimed protections against misuse cannot be achieved by encrypting the content. Encryption would not prevent the content from being accessed, copied, distributed, or stored. For these types of protection, "access control" is necessary. More particularly, the Big Book describes only the complete "invention" as providing such protection against the threats identified in the Big Book. In other words, by promising the type of effective access control protection said to be provided only by the complete VDE, these claims invoke that "invention."

MS Br., 17:4-14.

This passage is typical of Microsoft's reasoning. First, it is almost entirely devoid of evidentiary citations. The only citation that Microsoft makes is to four pages of Dr. Reiter's deposition testimony, testimony that Microsoft has not even put into evidence (it is excluded from the Keefe Decl.). Microsoft's failure to provide this testimony to the Court is understandable, since Microsoft has grossly mischaracterized the passage, in which Dr. Reiter explicitly disclaimed any requirement of absolute protection. Reiter II, 177:18-178:11. Declaration of Jeff McDow in Support of InterTrust's Claim Construction ("McDow Decl."), ¶ 2 and Ex. A.

Moreover, this passage is typical of Microsoft's arguments, since it piles inference on inference, none of them supported in any manner. Microsoft's chain of reasoning is as follows:

(1) The claims use the words "allows" and "determining," and do not qualify them.

(2) The absence of qualification means that the protections must be effective "no matter what effort may be made to take the unauthorized action." Microsoft makes this allegation, but does not even allege that one of ordinary skill in the art would have understood the apparently innocuous terms "allows" and "determining" to require absolute protection.

(3) The requirement of absolute protection means that the controls must be "effective in the face of the attacks identified in the Big Book." Microsoft makes no allegation that every

attack described in the patent specification is relevant to these particular claims (e.g., music downloading), nor does it explain why every possible attack must be protected against.

(4) The requirement of absolute protection against all types of attacks "cannot be achieved by encrypting the content. Encryption would not prevent the content from being accessed, copied, distributed or stored." Again, Microsoft presents no evidence for this proposition. Why, for example, would encryption not prevent content from being "accessed?" Microsoft doesn't say. Moreover, the claims themselves don't say anything about either the presence or the absence of encryption, and InterTrust has never alleged that the claims require encryption (nor that they exclude encryption for that matter).

(5) Since encryption is not sufficient, "[f]or these types of protection, 'access control' is necessary." The claims do not mention "access control." No Microsoft witness testifies that one of ordinary skill in the art would have understood these claims as requiring "access control." Instead, Microsoft imports "access control" into the claims because "access control" is allegedly better than encryption (also not mentioned in the claims) at ensuring the absolute degree of protection (also not mentioned in the claims) allegedly required by "allows" and "determining."

(6) Since access control is required, the claims invoke VDE:

Microsoft's argument reaches its conclusion in the following passage:

> More particularly, the Big Book describes only the complete "invention" as providing such protection against the threats identified in the Big Book. In other words, by promising the type of effective access control protection said to be provided only by the complete VDE, these claims invoke that "invention."

MS Br., 17:11-14.

This is a masterpiece of conclusory reasoning. "Such protection" is not mentioned in the claims, but is implied by Microsoft. The "threats identified in the Big Book" are not mentioned in the claims, but are implied by Microsoft. The claims do not make any type of "promise." This is implied by Microsoft. The claims do not mention "access control," either "effective" or non-effective. This is implied by Microsoft.

All of this, it should be recalled, rests on a rather thin reed: the presence of the words "allows" and "determining," in the claims, yet Microsoft provides no basis for concluding that

one of ordinary skill would have interpreted these terms as implying hundreds of VDE limitations.

2. '683, claim 2.

Microsoft's justification for concluding that 683.2 should be interpreted as requiring the "hundreds" of VDE limitations is the following

> This claim [683.2] also concerns a multi-node distribution system. Here, "secure containers" and "secure container rules" are distributed amongst various nodes. The claim appears to promise the ability to prevent access to or use of protected information, using the secure containers, secure container rules, and a "protected processing environment." (See Second Mitchell Decl. at 6-7). These protections are not qualified as to the nature or severity of the threat being faced; they impliedly are effective against all threats identified in the patent or Big Book. The only system described in the Big Book or '683 Patent said to accomplish such protections, is the complete VDE. This claim further invokes VDE by using VDE and vague terminology, such as "secure container" and "protected processing environment."

MS Br. 17:27-18:1.

The only support cited by Microsoft for this characterization of 683.2 is the Second Mitchell Decl. at 6-7. Those Declaration pages do not discuss this claim.

Microsoft's key argument is the following: "These protections are not qualified as to the nature or severity of the threat being faced; they impliedly are effective against all threats identified in the patent . . . ." Microsoft does not explain why an absence of qualification means the claims require the highest degree of security (as opposed to the lowest, or to the security relevant under the circumstances). Nor does Microsoft explain how this implication can be squared with specification statements that security may be limited, may be broken, or may consist of fewer than all protection mechanisms. JCCS Ex. C, 19(A)-(N), 19(Q)-(T).

3. '721, Claims 1 and 34.

Again, Microsoft's argument consists entirely of conclusory allegations. Microsoft argues that "The '721 Patent purports to improve the Big Book VDE by preventing the use of executable code (specifically "load modules" in Claim 1) except as authorized." MS Br., 18:8-9. No citation is given for this assertion, and Microsoft makes no attempt to tie it to the claims, other than noting that 721.1 recites load modules.

.. Microsoft continues by alleging that "Such prevention requires an access control capability." MS Br., 18:9-10. Again, no citation is provided, and neither claim mentions any such capability.

Microsoft then argues that the claims "promise such protections without any qualification." MS Br., 18:10-11. The claims contain no such promises, and Microsoft fails to explain why an absence of qualification requires the highest possible degree of protection.

Microsoft ends by arguing that the claims "invoke the 'invention'" by including the terms "protected processing environment," "tamper resistant barrier" and "security." As is discussed above, the first two of these are described using higher-security and lower-security embodiments, so these terms hardly support a requirement that the claims be interpreted using the highest possible security level. As to the word "security," this is a common word, and Microsoft provides no basis for reading a requirement of "VDE" into this term, other than the implication that VDE is the "context," an argument that is inconsistent with the multiple embodiments disclosed in the patents.

4. Other claims.

Microsoft's arguments regarding the other claims suffer from the same infirmities and should be rejected for the same reasons as discussed above.

E. Microsoft's Bases for Reading the Specification Into the Claims Are Either Mischaracterized or Do Not Apply.

Microsoft identifies various situations in which Microsoft believes that limitations can be read from the specification into the claims. MS Br. at 11:27-14:15. These situations are either mischaracterized by Microsoft or have no relevance to this case.

(1) To provide clarity. Microsoft cites cases for the proposition that, if a particular claim term deprives the claim of clarity, the court may look to the specification for guidance in interpreting the claim. MS Br., 11:27-12:13. Each of the cases cited by Microsoft concerned a particular interpretation issue raised by a particular claim element (e.g., does "automation code" mean particular code in an operating system? (Altiris, Inc. v. Symantec Corp., 318 F.3d 1363, 1374-75 (Fed. Cir. 2003)); does "coupling" require different voltages? (NeoMagic Corp. v.

Trident Microsystems, Inc., 287 F.3d 1062, 1071-72 (Fed. Cir. 2002)); does "sealingly connected" require misaligned taper angles? (Watts v. XL Sys., Inc., 232 F.3d 877, 882-83 (Fed. Cir. 2000)); does "without significant cross-linking" include a particular type of cross-linking? (North Am. Vaccine v. American Cyanamid Co., 7 F.3d 1571, 1575-76 (Fed. Cir. 1993)). [5]

None of these cases involved an attempt by a patent defendant to read hundreds of limitations into every claim, nor to interpret numbers of claim terms using significant limitations that are not tied to any use of the terms themselves in the specification.

(2) Express or implied definition in the patent. Most of the cases cited by Microsoft involve an explicit definition in the patent or file history. Notably, where such definitions have been provided in the present case, Microsoft has chosen to ignore them (e.g., Device Class, Contained).

As Microsoft points out, the cases involving an "implied" definition concerned use of a claim term "throughout the entire patent specification in a manner consistent with only a single meaning." MS Br., 12:19-20. In this case, however, Microsoft makes no attempt to establish that any particular claim terms are used consistently with only one meaning. Indeed, Microsoft regularly notes that the specification uses claim terms in multiple manners, or in a manner inconsistent with Microsoft's proposed interpretation (e.g., "tamper resistant barrier," "protected processing environment").

(3) Important to the Invention. This issue is addressed in InterTrust's opening brief. That specification characterizations of "the invention" do not constitute a magic formula automatically pulling the specification into the claims, however, is made clear by the cases cited in InterTrust's opening brief, each involving specification statements about "the invention," each holding that those statements did not limit the claims. Microsoft does not even attempt to distinguish these cases.

Microsoft's characterization of SciMed Life Sys. v. Advanced Cardiovascular Sys., 242 F.3d 1337 (Fed. Cir. 2001) is at best disingenuous: "limiting claim term 'lumen' to 'coaxial

---

[5] One of the cases cited by Microsoft (Ethicon Endo-Surgery v. United States Surgical Corp., 93 F.3d 1572 (Fed. Cir. 1996)) is miscited, since the Federal Circuit used the prosecution history,

lumen' in part because the specification characterized the coaxial configuration as part of the 'present invention.'" MS Br., 13:7-9. In fact, as InterTrust pointed out in its opening brief, the Scimed patent went well beyond characterizing this element as "part of" the invention: the specification stated that the element was present in **"all embodiments"** of the invention, a statement the Federal Circuit characterized as "the most compelling portion of the specification," a statement that significantly exceeds anything present in the current case. 242 F.3d at 1343.

In addition, the cases cited by Microsoft involved specific issues relating to specific terms (Scimed: does "lumen" mean "coaxial lumen?"; Toro Co. v. White Consol. Indus., 199 F.3d 1295, 1300-01 (Fed. Cir. 1999): does "including" mean "attached?"). Neither case held that statements about the "invention" required that an entire embodiment with hundreds of limitations be incorporated wholesale into every claim.

(4) Distinguishing prior art. Microsoft argues that statements distinguishing prior art may support reading embodiments into the claims. MS Br., 13:10-20. Cases cited by Microsoft generally concern file wrapper estoppel, Spectrum Int'l v. Sterilite Corp., 164 F.3d 1372, 1378 (Fed. Cir. 1998); Rheox, Inc. v. Entact, Inc., 276 F.3d 1319, 1325-26 (Fed. Cir. 2002).[6]

The one case cited by Microsoft that does relate to a specification statement illustrates why this doctrine does not apply in the present case. In Innovad, Inc. v. Microsoft, 260 F.3d 1326 (Fed. Cir. 2001), the court construed the claim term "dialer" in light of a specification statement that prior art dialers of a particular type were "useless" for a particular purpose. On that basis, the court concluded that the claim term "dialer" should exclude that particular type.

Here, in contrast, Microsoft points to no specification statement discussing a specific claim term in light of the prior art. For example, there are no specification statements to the effect that prior art software tamper resistant barriers were inadequate for some particular purpose. Nor does Microsoft cite any case standing for the proposition that a general statement about the inadequacies of the prior art and the advantages of an overall embodiment described in

---

rather than the specification, to interpret the claim element. 93 F.3d at 1579-80.

[6] CCS Fitness, Inc. v. Brunswick Corp., 288 F.3d 1359, 1366-67 (Fed. Cir. 2002) includes this factor in a list of possible factors but does not apply it, though it does cite the Spectrum file wrapper language.

the patent requires that every detail of that embodiment be read into every claim. Nor does Prof. Mitchell's testimony about various references fill this gap, since he does not tie his discussion of these references to any particular specification statement that distinguishes them. Mitchell 2nd Decl., 10:17-18:4.

(5) Express disclaimer. Microsoft does not argue that any express disclaimer exists.

F. Microsoft's Argument about the InterTrust Divisionals Misses the Point.

In its opening brief, InterTrust pointed out that the Patent Office's restriction requirement demonstrated that the foundational InterTrust application involved multiple inventions, inventions that the Patent Office expressly held related to separate classes, each shown to be "separately usable." InterTrust Opening Br., 11:5-12:20. This determination rebuts any argument that the original InterTrust specification disclosed only a single VDE "invention."

Microsoft makes arguments in response, but none to the point. Microsoft argues that the Patent Office's restriction requirement is irrelevant because "InterTrust's patent claims are free to recite additional features, which additional limitations may (or may not) make them separate 'inventions' under Patent Office restriction practice. But, that is not the issue here." MS Br., 15:3-7.

Microsoft does not explain why "that is not the issue here," and it certainly seems to be the issue: Microsoft argues that the patents disclose a single, unitary VDE invention, and hundreds of limitations must be read into every claim. Microsoft relies heavily on statements referring to "the invention," and argues that "the invention" must be incorporated into every claim. The restriction requirement, however, makes it clear that references in the application to "the invention" cannot be read as meaning that the application recited a single invention.

Microsoft also points out that divisional patents may end up with claims directed to the same invention, and that in such a case the resulting patents are invalid. Microsoft further argues that, because the claims of the divisional applications were changed, the presumption they were directed to different inventions should not apply, citing Gerber Garment Tech., Inc. v. Lectra Sys. Inc., 916 F.2d 683 (Fed. Cir. 1990).

Gerber includes no such holding, nor could it, since the presumption of patent validity is statutory, and cannot disappear merely because a divisional application's claims have been changed. The Court must presume that the Patent Office acted properly in the original restriction requirement, and in issuing the subsequent patents, including the amended claims. Thus, the Court must presume that the divisional applications were originally drawn to different inventions, and that the subsequent patents issuing from those applications were also drawn to different inventions, since otherwise the divisional patents would be invalid, and those patents carry a statutory presumption of validity.

Microsoft characterizes Ballard Med. Prod. v. Allegiance Healthcare Corp., 268 F.3d 1352 (Fed. Cir. 2001), as follows: "limiting claims of both a patent issued from the parent application and a patent issued from a divisional of such parent to exclude a particular type of valve based on statements made in common specification text and prosecution history of the parent application." MS Br., 15:26-16:2. This is wrong. In Ballard, the Federal Circuit held that statements in a parent prosecution history can serve to limit later patents. 268 F.3d at 1361-62. No issue of statements made in the specification was raised in the case. In particular, the Federal Circuit did not address specification statements about "the invention."[7]

G. Individual Claim Elements.

1. Microsoft ignores ten claim elements.

Microsoft filed a forty page brief, plus two expert Declarations, but neither Microsoft nor its experts have anything to say about ten of the thirty terms at issue in this hearing: (1) Aspect, (2) Authentication, (3) Compares, (4) Derive, (5) Designating, (6) Device Class, (7) Digital Signature/Digitally Signing, (8) Executable Programming/Executable; (9) 721.1: "digitally signing a second load module...." (10) 912.8: "identifying at least one aspect of an execution space required for use and/or execution of the load module."

[7] Moreover, Ballard involved claims interpreted under 35 U.S.C. § 112(6), which are supposed to be limited to the embodiments disclosed in the specification, so this case would be distinguishable even if Microsoft had correctly characterized it. 283 F.3d at 1359-60.

2. **Use.**

InterTrust's definition is taken from a standard dictionary (JCCS, Ex. C, 23(A)). The Federal Circuit approves using dictionary definitions. Inverness Med. Switz. GmbH v. Princeton Biomeditech Corp., 309 F.3d 1365, 1369-70 (Fed. Cir. 2002).

Microsoft's argument on "use" is mysterious, as Microsoft concentrates on "encryption," and on a series of alleged InterTrust contentions. MS Br., 20:6, 21:20-25. Encryption appears irrelevant to the proposed definitions, and InterTrust never made the contentions.

3. **Copy.**

Microsoft responds at length to arguments never made by InterTrust, and ignores InterTrust's central point: Microsoft's definition would result in a nonsensical interpretation of 193.1, in which a budget for making copies would be used up by "phantom," internal reproductions that the user would never know existed, much less be able to use. Microsoft does not attempt to explain how its interpretation would make sense in the context of the claim.[8]

4. **Secure/Securely.**

Microsoft acknowledges that its proposed definition is neither "standard" nor an express definition from the patent. MS Br. at 28:6-7. What Microsoft fails to acknowledge is that its definition actually contradicts the specification. According to Microsoft, a system is secure only if it protects five separate properties against attack, and only if this protection is 100% effective. As described above (§ II A 2), however, the specification explicitly describes various levels of security, and characterizes them all as "secure."

Microsoft attacks InterTrust's definition, arguing that InterTrust ignores the effectiveness of the efforts taken. MS Br., 26:10-11. In fact, InterTrust's proposed definition requires that the mechanisms employed "prevent," "detect" or "discourage" misuse or interference. A mechanism that fails to perform these functions (e.g., a completely ineffective mechanism) would not be "secure" under InterTrust's definition.

[8] Prof. Mitchell's commentary on "copy" is similar: a great deal of discussion of this phrase in the abstract, but no attempt to explain how Microsoft's proposed definition would make sense in the context of the claim, nor any attempt to respond to InterTrust's discussion of this in its opening Brief. Mitchell 2nd Decl., 6:23-8:2.

Microsoft also argues that VDE "promises the ability to prevent" various types of misuse, and that detecting or discouraging misuse is not security. MS Br. at 26:14-20. Microsoft cites no support for this proposition, and it is clearly incorrect. In some circumstances, mechanisms that allow the detection of misuse are fully sufficient for security. For example, technology that made it possible to detect an alteration of a driver's license would render the driver's license "secure," since, although the driver's license could be altered (e.g., to change the birthdate of an underage would-be drinker), the fact that the change could be detected would make it impossible for an attacker to gain any benefit from the misuse.

Thus, one disclosed embodiment of the tamper-resistant barrier "detects tampering and/or destroys sensitive information." JCCS Ex. C, 22(A). It is impossible to read this passage of the specification as requiring any protection mechanism other than "detection."

Microsoft also mischaracterizes Dr. Reiter's testimony, alleging he testified that none of the five listed forms of protection is required. MS Br., 27:1-3. As with so many of Microsoft's citations, however, this one is false. In the cited passage from Dr. Reiter's deposition, a Microsoft attorney asked a series of questions, each question relating to a single mechanism. Since security requires one or more of these mechanisms, but does not require all of them, Dr. Reiter correctly answered "no" when asked whether the claims required each mechanism in isolation. Dr. Reiter was never asked whether at least one mechanism from the entire group was required, and he never testified that security could exist without any mechanism at all. Reiter 202:5-204:14 (McDow Decl., Ex. A.)[9]

5. Secure Container.

Microsoft alleges that only a single embodiment is disclosed, and that it requires the ACCESS method. MS Br., 29:10-13. This is false. The ACCESS method excerpts quoted by Microsoft are part of a longer passage that is expressly described as being an "an example" ('193 patent, 192:2), and the same passage describes the ACCESS method Microsoft cites as a

---

[9] Similarly, suppose a movie theater offered half-price tickets to customers ages ten to twelve, and a particularly obtuse customer posed the following series of questions: "Do I have to be 10 to receive the discount?" "Do I have to be 11 to receive the discount?" "Do I have to be 12 to receive the discount?" The answer to all three questions would be "no," but this obviously

"complicated procedure" and notes that "in many cases" a "relatively trivial" procedure may be used instead. Id. at 192:6-11.

In addition, Microsoft argues that the "access control ability of VDE secure containers" is "critical to VDE's promise to content owners." MS Br., 28:3-7. The phrase "VDE secure container" does not appear in the '193 patent. McDow Decl., ¶ 3. When the inventors wanted to refer to a container in terms of VDE capabilities, they explicitly identified it as a "VDE container" (e.g., JCCS Ex. C, 20(E)). The patent claims do not refer to "VDE containers," but instead refer to "secure containers."[10] Microsoft seeks to confuse this issue by using the phrase "VDE secure containers," in an apparent attempt to mislead the Court into believing that "secure containers" and "VDE containers" are identical.[11]

6. Tamper Resistant Barrier.

As discussed above, Microsoft's construction of "tamper resistant barrier" admittedly excludes an embodiment that is referred to in the specification as a "tamper resistant barrier." Microsoft's argument also suffers from other defects. Microsoft alleges that the specification requires a hardware barrier wherever content is "assigned usage control information, or used." MS Br. at 33:10-14. Microsoft quotes several excerpts at length, none of which even mentions tamper resistant barriers, much less excludes software tamper resistant barriers.

Moreover, the term "tamper resistant barrier" is recited only in 721.34. Microsoft rather casually alleges that "all of the mini-Markman claims contemplate one or both of these two conditions" (i.e., assigning usage control information to content or using content). MS Br., 33:10-12. Claim 721.34 has no reference to assigning usage control information or any use of content, nor does it have any language from which such elements can be inferred.

---

wouldn't establish that the discount is an illusion.

[10] InterTrust agrees that "VDE containers" are one embodiment of "secure container," but this obviously does not mean that all "secure containers" are "VDE containers."

[11] Prof. Maier states that "I believe it is apparent that [secure container] is intended to refer to the VDE container." Maier Decl., 22:17-18. He gives no basis for this belief, nor does he explain how "secure container" is used in the specification, other than noting it only occurs twice in the '193 patent. This statement is itself misleading, since it ignores the extensive use of the term in the '683 and '861 patents, both of which include mini-Markman claims using "secure container." McDow Decl., ¶ 5.

In addition, Microsoft's argument that a hardware barrier is required ignores alternative embodiments described in the specification. For example, Microsoft ignores the excerpt cited by InterTrust at JCCS Ex. C, 22(B), which describes a "secure HPE" with a software tamper resistant barrier, and states that "Any service may be provided by such a secure HPE . . . ."

Prof. Maier alleges that the "tamper resistant barrier" recited in the claims is referred to as a "tamper resistant security barrier," or a "tamper-resistant hardware security barrier." Maier Decl. 34:21-23. The claim uses the term "tamper resistant barrier," rather than these other phrases. That the specification uses these other phrases to refer to hardware barriers is evidence that the unqualified phrase "tamper resistant barrier" should apply to both embodiments.

Prof. Maier acknowledges that the patent "alludes to" a software tamper resistant barrier, but he states that "the specification gives no indication how to determine what the boundaries of such a 'barrier' might be or how to implement such techniques successfully." Maier Decl., 35:7-10. The quotation (JCCS Ex. C, 22(B)) contains more than an "allusion" to a software tamper resistant barrier, it explicitly describes numerous techniques that may be used to provide one.

7. Protected Processing Environment.

Microsoft's main argument regarding this term is discussed above in § II B 2, and its other arguments amount to quibbles that InterTrust's definition is not specific enough. No claim construction can address every possible infringement issue. As the Federal Circuit has held, if a claim term is reasonably defined in general terms, it is the Court's obligation to adopt that construction, leaving the question of application of the general definition to the jury. PPG Industries, 156 F.3d at 1354-55.

8. Component Assembly.

Microsoft asserts that "In the Big Book the term 'component assembly' (also called 'component') uniformly is used to refer to executable components, which are an assembly of independent, executable load modules and data." MS Br. at 35:12-14. Microsoft provides no support for the assertion that a "component assembly" is also called a "component," an assertion that seems odd, since a "component assembly" is self-evidently an assembly of components.

Microsoft's main argument is that InterTrust's definition would allow the possibility of a component assembly that does not include any executable code. InterTrust did not intend to leave open the possibility that a component assembly might include no programming. InterTrust is willing to amend the third sentence of its proposed construction to read as follows: "Component Assemblies must include code, and are utilized to perform operating system and/or applications tasks."

Microsoft makes no attempt to otherwise defend its complicated definition.

Prof. Maier's discussion of "component assembly" notes that the specification describes multiple embodiments (Maier Decl., 17:1-3), but appears to consider this to be an improper practice. At a later point in his Declaration, Prof. Maier states that InterTrust's citations relating to "component assembly" all relate to VDE, though he only quotes language from two of these citations. Maier Decl., 27:2-10. Prof. Maier appears not to have appreciated the point of a number of these quotations: that the VDE-related description of "component assembly" is expressly and repeatedly referred to as a "preferred embodiment."

9. Control (noun).

Microsoft's argument includes an analogy relating to librarians, but without any support from the experts or the patents that this analogy is reasonable or correct. Thus, Microsoft argues that "rules" and "controls" should not be equated, on the basis that "rules" are non-executable, whereas controls are "executable." Microsoft presents no evidence for its assertion that "rules" are non-executable, other than the argument that "rules" constitute the "guard" in Microsoft's analogy.

Moreover, the quotations cited by Microsoft in its brief and in JCCS Ex. D do not state that a "control" must be executable, but instead are merely consistent with "controls" being executable programming, as is InterTrust's proposed definition.

Prof. Maier argues that "control" should be interpreted in light of VDE because 75% of the passages cited by InterTrust allegedly relate to VDE. Maier Decl., 28:2-3. Prof. Maier does not explain the significance of this statistic, and it does not seem to have occurred to Prof. Maier that the non-VDE uses constitute evidence that the term should not be limited to VDE.

10. A budget specifying the number of copies which can be made of said digital file (193.1).

Microsoft argues that InterTrust's construction does not specify "since when," "by whom" or "by what." The claim does not require this information, and Microsoft does not explain why a budget must include it.

11. Container.

Although Microsoft discusses this word separately (MS Br., 39:3-7), "container" is not a disputed term, but instead occurs as part of "secure container." InterTrust's definition of "secure container" rests on a definition of "container" from the Microsoft Computer Dictionary and is consistent with use of the term in the mini-Markman patents, and a contemporaneous Microsoft patent. JCCS Ex. C, 20(I), (J).

Microsoft argues that, in the patents, "container" is not used in the manner asserted by InterTrust, citing Alexander Decl. 20(A)-(D). Microsoft provides no explanation for why these passages are inconsistent with InterTrust's construction.

12. Containing.

The patent explicitly defines "containing" as including referencing. JCCS Ex. C, 7(B). Microsoft's argument about the "ordinary meaning" of the term is both unsupported and irrelevant in light of this explicit definition, and in light of the Microsoft Computer Dictionary definition for "container" ("a file containing linked or embedded objects"). JCCS Ex. C, 20(I).

13. Control (verb) / Controlling.

InterTrust's definition comes directly from a standard dictionary. Microsoft's only response is that this is inconsistent with VDE. Microsoft fails, however, to cite any text from the patents defining "controlling" in any particular manner, and the only quotation it includes does not even use "control" as a verb. As InterTrust pointed out in its opening brief, the patents use "control" as a verb in many non-VDE contexts. InterTrust Opening Br., 21:23-28.

14. "Controlling the copies made of said digital file" (193.1).

Microsoft does not attempt to support its proposed definition, which is long and complex. Instead, Microsoft quibbles about implications arising from InterTrust's construction.

The InterTrust construction is based on the manner in which this phrase is used in the claim, in which it explains the "copy control." See JCCS Ex. A, Row 7. The nature of the copy control is further described later in the claim. JCCS Ex. A, Rows 8 and 9. InterTrust's definition is based on the phrase itself and on its context in the claim, a context Microsoft entirely ignores.

15. "Derives information from one or more aspects of said host processing environment" (900.155).

Microsoft's argument consists of unsupported allegations, including the assertion that a "unique" signature is required, that "the derived information may serve no security purpose at all," and that this "is contrary to the patent." Microsoft's Ex. D evidence for this term consists of 122 separate citations amounting to twenty pages. Since Microsoft's allegations are not tied to any particular text, InterTrust cannot respond, other than stating that any text Microsoft may subsequently identify will simply be an embodiment, since this term occurs frequently in the passages quoted in Microsoft's JCCS Ex. D.[12]

16. Host Processing Environment.

In its opening brief, InterTrust acknowledged that its definition of Host Processing Environment does not include the "insecure" variant, and proposed an alternate definition. InterTrust Br., 36:13-19. Microsoft ignores this, criticizing InterTrust for failing to cover insecure host processing environments. MS Br., 40:10-13. Microsoft otherwise fails to respond to any of InterTrust's points on Host Processing Environment. InterTrust Br., 36:20-37:10.

17. Identifier.[13]

Microsoft claims that InterTrust's definition of "identify" is "contrary to the ordinary meaning." InterTrust's definition is from the American Heritage Dictionary. JCCS Ex. C, 17(F).

---

[12] If Microsoft subsequently identifies particular relevant passages, InterTrust will move to strike those identifications as being inconsistent with this Court's Patent Local Rules. It is one thing to make assertions that are supported by one or two pages of quoted text. It's quite another to make general arguments that are not supported by any individual citations but are instead allegedly supported by twenty pages of block quotes. The Patent Local Rules require the parties to identify relevant evidence. Twenty pages of unexplained quotes do not comply with this requirement.

[13] Microsoft's brief discusses "identifying (identify)," neither of which are terms to be construed in this proceeding. MS Br., 40:14. Since Microsoft also cites the JCCS Ex. A reference covering "identifier," InterTrust will assume that Microsoft is intending to discuss this term, and will respond accordingly.

18. Tamper Resistance.

Microsoft's argument consists of an unsupported assertion ("plainly is not what VDE means by 'tamper resistance'") and a quibble ("more than difficult [sic] than what?"). MS Br., 40:21-25. As to the former, assertions do not constitute evidence supporting Microsoft's construction. As to the latter, more difficult than if the tamper resistance were not present.

Prof. Maier, on the other hand, spends considerable time discussing this concept, including two pages of symbolic logic, apparently intended to prove that tamper resistance cannot include detection of tampering. Maier Decl., 32-34. However, whatever the details of Prof. Maier's analysis, he simply fails to address JCCS Ex. C 21(B), a quotation that explicitly states that a tamper resistant barrier "detects tampering and/or destroys sensitive information." This quotation clearly equates tamper resistance with detecting tampering, and does not require that tampering actually be blocked.

19. Budget.

Although Microsoft's brief does not refer to "budget," Prof. Maier's Declaration discusses this term, though without any citation to the claims or specification. Maier Decl., 17:6-13. Prof. Maier acknowledges that the specification sometimes uses "budget" to refer to data and in other places uses "budget" to refer to executables, but treats this as an "inconsistency" that leads to "confusion" (Maier Decl., 17:11) rather than as multiple embodiments that establish the term can refer to either data or an executable.

20. Clearinghouse.

Prof. Maier alleges that "clearinghouse" has "a specific meaning in the banking and commerce fields." Maier Decl., 24:1-2. Unfortunately, he fails to explain what this alleged meaning might be, or how it would support reading VDE features into the claims. Instead, he cites some quotations from InterTrust, but does not respond to a primary point made in InterTrust's opening brief: Visa and AT&T are identified in the specification as "clearinghouses," yet no one could believe that either Visa or AT&T have the various VDE features required by Microsoft's proposed definition.

H. Testimony Cited by Microsoft.

Exhibit A to the Keefe Declaration contains numerous quotations that Microsoft does not refer to in its brief. Most of these quotations are from inventors or third party deponents. The inventor testimony is not tied to the patents, and "The subjective intent of the inventor when he used a particular term is of little or no probative weight in determining the scope of a claim (except as documented in the prosecution history)." Markman v. Westview Instruments, Inc., 52 F.3d 967, 985-86, aff'd, 517 U.S. 370 (1996). The third party testimony suffers from the same defects as the testimony InterTrust moved to strike in connection with Microsoft's summary judgment motion, and is incompetent for those same reasons.

III. CONCLUSION.

Microsoft's VDE-centric claim interpretation would require the Court to ignore embodiments disclosed in the specification, and to interpret particular claim terms in a manner that excludes disclosed embodiments, a practice the Federal Circuit has held is "rarely, if ever," correct. Microsoft supports this extreme position with conclusory reasoning and egregious miscitations of the record.

Microsoft's claim constructions are longer and more complicated than any constructions ever adopted by any court. Those constructions would read literally hundreds of limitations into every single claim. InterTrust respectfully requests that the Court reject Microsoft's VDE-centric interpretation position and adopt the claim constructions proposed by InterTrust.

Dated: April 21, 2003

Respectfully submitted,

DERWIN & SIEGEL, LLP

By: ______________________

DOUGLAS K. DERWIN
Attorneys for Plaintiff
INTERTRUST TECHNOLOGIES CORPORATION

WILLIAM L. ANTHONY (State Bar No. 106908)
ERIC L. WESENBERG (State Bar No. 139696)
KENNETH J. HALPERN (State Bar No. 187663)
ORRICK, HERRINGTON & SUTCLIFFE, LLP
1000 Marsh Road
Menlo Park, CA 94025
Telephone: (650) 614-7400
Facsimile: (650) 614-7401

STEVEN ALEXANDER (admitted *Pro Hac Vice*)
KRISTIN L. CLEVELAND (admitted *Pro Hac Vice*)
JAMES E. GERINGER (admitted *Pro Hac Vice*)
JOHN D. VANDENBERG
KLARQUIST SPARKMAN, LLP
One World Trade Center, Suite 1600
121 S.W. Salmon Street
Portland, OR 97204
Telephone: (503) 226-7391
Facsimile: (503) 228-9446

Attorneys for Defendant and Counterclaimant,
MICROSOFT CORPORATION

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

OAKLAND DIVISION

INTERTRUST TECHNOLOGIES CORPORATION, a Delaware corporation, Plaintiff, v. MICROSOFT CORPORATION, a Washington corporation, Defendant.	Case No. C 01-1640 SBA (MEJ) Consolidated with C 02-0647 SBA (MEJ) **REPLY TO INTERTRUST'S OPPOSITION TO MICROSOFT'S BRIEF IN SUPPORT OF MOTION FOR SUMMARY JUDGMENT THAT CERTAIN "MINI-*MARKMAN*" CLAIMS ARE INVALID FOR INDEFINITENESS**
MICROSOFT CORPORATION, a Washington corporation, Counterclaimant, v. INTERTRUST TECHNOLOGIES CORPORATION, a Delaware corporation, Counter Claim-Defendant.	

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Federal Cases

FEDERAL STATUTES

I. INTRODUCTION AND SUMMARY OF ARGUMENT

InterTrust's opposition brief throws up a storm of noise, diversion and straw arguments that should not distract this Court's attention from the very simple question on which the defense of indefiniteness will be determined: Whether the claim has sufficiently definite scope that a person of ordinary skill in the art can understand what it means in light of the specification and thereby determine what is outside its scope. *Union Pac. Resources Co. v. Chesapeake Energy Co.*, 236 F. 3d 684, 692 (Fed. Cir. 2001). For each of the eleven claims challenged on this motion, the answer must be, "No."

What emerges from InterTrust's opposition brief are two important points upon which the parties agree: First, "secure" is a relative term that has only a vague, general meaning in the art, which can mean different things in different contexts. Second, to determine what is "secure" in any particular context one of skill in the art needs specific criteria. The essential problem with InterTrust's patents is that they fail to provide the needed context and they fail to adopt any particular criteria, leaving both critical steps for others to guess at. They further fail to define "secure" expressly, and they fail to define it implicitly by identifying any particular technology used to achieve security. When one turns to the Big Book for resolution of the resulting ambiguity, it is like coming to a trailhead with 50 signs labeled "secure," but each pointing in a different, inconsistent, and often times contradictory direction.

The term "secure" is unusual in that it is a label characterizing a multidimensional condition of something – a result achieved amid constantly changing circumstances. It is an inherently subjective concept that can be evaluated in many different ways (with correspondingly different outcomes). Labels set forth in patent claims, however, must be subject to an objective evaluation. Otherwise, it is impossible for the public to evaluate the scope of the claim.

The ***claims*** fail to recite either context or criteria. The traditional places to which one turns to correct this shortcoming are equally unavailing. The evidence from the parties' experts, corroborated by third party accounts, confirms that definite context and criteria is critical information for anyone having skill in this art, and it is information that merely having skill in the art does ***not provide***. To the contrary, persons of skill in the art are aware of a multitude of

possible ways of distinguishing between something that is "secure" and something that is "not secure." Finally, ***the specification*** is equivocal on everything except what "VDE" can do, and the file history offers no resolution. Indeed, the specification compounds the problem because it mentions but fails to adopt any of the many possible security contexts and criteria. After reading the nearly one thousand pages of Big Book text, the person of ordinary skill in the art would have no idea what, for example, a claim's "secure container," "secure memory," or "secure process" must protect, or against what threats, or to what degree, or by what criteria such evaluations should be conducted. The evidence from the parties' experts, corroborated by third party accounts, confirms that specific context and criteria are critical information for anyone having skill in this art, and it is information that merely having skill in the art does ***not provide***. It is for these reasons that the mini-*Markman* claims are indefinite and should be declared invalid.

II. "SECURE" AS USED IN THESE MINI-MARKMAN CLAIMS RENDERS THEM INDEFINITE

A. A Person of Skill Reading the Claims Cannot Tell What "Secure" Means in Light of the Relevant Art

One of skill in the art reading the claims finds references to "secure memory," "secure database," "secure container," "securely assembling," and "level of security," but no explanation of what is meant by "secure" other than the promises made for the "present invention," "VDE." Looking to the art as a whole for guidance offers no comfort. The term, *as InterTrust admits*, has only a very general meaning – that some designs, techniques or mechanisms are used to protect certain properties against some kind of attack or adversarial conditions. InterTrust Opp., at 4 (quoting Prof. Mitchell's definition as the one on which both parties' experts "agree"). This definition manifestly lacks a clear boundary. Which designs, techniques, mechanisms, properties, attacks, and or conditions are intended? The claims point to no criteria in the art that would answer that question.

Both parties' experts agree that criteria are needed to reach a precise understanding of "secure." The testimony of InterTrust's own expert, cited in Microsoft's opening brief, fully supports the proposition that the term needs further specification of parameters and criteria in

order to be sufficiently definite.[1] Microsoft Brief, at 4. InterTrust's expert now adds that to apply the general meaning of "secure" "to a particular product or system, it is necessary to understand the context of that product or system." Reiter Decl., at ¶ 3. Dr. Reiter also admits that there are "several recognized methodologies for determining if computer products are 'secure'" and that "[c]omputer security professionals routinely use such methods to determine if products or methods are 'secure.'" Opp., at 3; Reiter Decl., at ¶ 3. InterTrust even approvingly characterizes Dr. Mitchell's testimony as meaning that one must know the protected properties and potential attacks to determine if a particular system is "secure," and that recognized methodologies are used to perform this investigation. *Id.* at 5. The Mitchell declaration, scholarly articles, and third-party witnesses have provided evidence to the same effect. *Id.*; Mitchell Decl., at 4-11.[2]

It should be noted here that InterTrust's allegation that Prof. Mitchell did not try to understand the terms in the context of the claims is based on a misrepresentation of his testimony. As Prof. Mitchell clearly explained, for each term and phrase in question, he "tired to look at its meaning in three different ways" – whether the term by itself has a commonly understood specific meaning, whether the term is clear "in the context of the claim," and whether the patent specification provides "any further information." (Mitchell Depo. at 294). In its brief, however, InterTrust cut off the quotation of Prof. Mitchell's testimony right before he gave an answer that contradicted the proposition for which InterTrust quoted him:

> A. I – I tried to explain a little bit earlier that my task to this point in this case has been to, first of all, understand the patent's specs and so on, and, second, in particular to this declaration, think about these particular phrases, what they mean in general, what they appear to mean in the claims, and ponder the question of whether the specification gives us additional useful information so that I could pin down the meaning of these terms in a useful and meaningful way.

---

[1] InterTrust erects Prof. Mitchell's effort to summarize the different axes of security into a classic straw man. Calling it a "test" – a term nowhere used by Microsoft – InterTrust reasons that, because this "test" is not recognized as such in the art, it sheds no light on the definiteness of InterTrust's patent claims.

[2] For this reason, InterTrust's lengthy argument that "secure" has a meaning in the art is beside the point. InterTrust Opp., at 2-3. As Microsoft stated in its opening brief, "while communicating a general or conceptual meaning, the term 'secure' lacks any precise, uniform definition to inform a person of skill in the art what it means *unless a number of questions are answered.*" Microsoft's Brief in Support of Motion, at 3 (emphasis added).

> In that process, I have read the claims and have some understanding of what they appear to promise and what they seem to mean in general. But as far as doing further detailed analysis of what is exactly required by each claim, I haven't really studied that in -- in a proper way yet.

Wesenberg Reply Decl., Exh. A (Mitchell Depo., Vol. 2, at 299:1-17).

Because the challenged claims use "secure" without providing specific parameters or criteria or referencing any in the art, one cannot determine their scope by reading them. A person of ordinary skill is left unable to define "secure" in light of the art and thus unable to understand the claims precisely enough to know what is in their scope.

B. <u>The Specification Does Not Select Any Criteria for Evaluating "Secure", Though It Refers to Some</u>

Faced with a vague and general "ordinary" meaning, we look to the patent specifications to see if they point to any of the criteria recognized in the art. InterTrust and Microsoft have identified some of the well-known "off-the-shelf" standards for determining "security," including the Common Criteria for Information Technology Security Evaluation, the Trusted Computer System Evaluation Criteria ("TCSEC"), and Federal Information Processing Standard 140-1 ("FIPS 140-1"). InterTrust Brief, p. 3; Reiter Decl., pp. 3-7. The fatal problem with InterTrust's specifications is that while they mention some of these standards, they adopt none of them. Nowhere is there a clear indication that a particular standard or identified criteria is the one to follow. The specification treats them as optional and applicable, if at all, only to a small part of the universe of the patent.

The TCSEC, for instance is mentioned in one column of the '193 patent, in a discussion of the possible use of VDE to support document management for a large organization. In a list of examples of how "VDE-enforced control capabilities" can be used to manage documents, the specification states that one particular type of document transmission channel and one type of storage device "could be" set up with restrictions that would satisfy the Device Labels requirement of the TCSEC. '193, col. 279:45-60. But these are just two examples (out of nine) of uses to which VDE can supposedly be put in one type of customer context, out of a great many others promised in the patent. Nowhere does the patent state or even suggest that TCSEC or any

part of it is meant to provide criteria to define "secure" throughout the patent, and interTrust does not make that argument now.

Likewise, the '721 specification mentions the FIPS-186 "Digital Signature Standard," but only as one possible methodology for evaluating the "security" of a digital signature. Again, InterTrust does not even argue that this is the standard a person of skill should use to evaluate whether something is "secure," but merely that one could do so.

C. The Specification Does Not Define "Secure" for Purposes of the Patent

Lacking a known criteria or a specified new criteria, an otherwise indefinite claim can be saved if the specification defines the proper measure of the problem term. Unfortunately, the 900+ pages of the patent specification point in so many different directions that it is impossible to know which apparent definition of "secure" to use. The patent does contain a great deal of verbiage about security methods and degrees. But its discussion of these issues is tantamount to a recitation of almost everything security could possibly mean or include, including unbounded references to whatever is not expressly recited in the patent.

1. The Specification Does Not Define "Secure" Explicitly

The patent never explicitly defines what "secure" means, either lexically or by outlining its own security policy or set of security criteria, a fact which InterTrust has not disputed.

2. The Specification Does Not Define "Secure" by Functional Description

The specification also fails to give "secure" a precise and unambiguous meaning by describing it functionally. That is, no clear and precise meaning of "secure" can be derived from the technological features disclosed in the specification. Although the specification contains a voluminous recitation of detail, that detail itself describes so many purportedly different levels of "security" that it is impossible to tell which technological features suffice to make a system "secure" in any particular instance. (As discussed below, it is inconsistent for InterTrust to argue that the specification provides the detail needed to make "secure" definite enough to determine what infringes, when it has excluded any such detail from its proposed Markman definition of the same term.)

The discussion of encryption mechanisms cited by InterTrust as supposed evidence of secure's definiteness exemplifies this. InterTrust argues that the '193 patent "contains a passage contrasting 'highly secure' encryption algorithms with 'extremely secure' algorithms, and explicitly identifies each type of algorithm, including explaining circumstances under which each should be used." InterTrust's opposition brief blithely reassures the reader that "both 'highly secure' and 'extremely secure' algorithms are 'secure.'" But these phrases clearly denote different degrees of security. To which level do the claims refer when they employ "secure"? InterTrust's answer that the specification tells one which "secure" mechanisms to use under which circumstances is untrue. The "highly secure" algorithm in this example is described simply as a "'bulk encryption/decryption technique.'" '193, col. 67:18-19. Elsewhere, the patent states that VDE "does not require any specific algorithm ... for bulk encryption/decryption." '193, Col. 201:27-29. More importantly, for both the "highly secure" and "extremely secure" cases, the measures mentioned are described as "preferable." *Id.*, col. 67:18, 21. This implies that there are circumstances under which the "preferable" option would not be employed, raising the question of what those circumstances are, who would make the decision, and how.

The next example cited by InterTrust begins to answer that question: in fact, "secure" is not evaluated by anything intrinsic to the patent, but by a subjective and unpredictable decisionmaking process. A discussion of encryption techniques that InterTrust offers as proof of the specificity with which the patent allegedly endows "secure," InterTrust Opp., at 6; '193, col. 201:63-202:12, is immediately preceded by this explanation:

> VDE 100 provided by the preferred embodiment accommodates and can use many different key lengths. The length of keys used by VDE 100 in the preferred embodiment is determined by the algorithm(s) used for encryption/decryption, ***the level of security desired***, and throughput requirements. Longer keys generally require additional processing power to ensure fast encryption/ decryption response times. Therefore, there is a tradeoff between (a) security, and (b) processing time and/or resources. Since a hardware-based PPE encrypt/decrypt engine 522 may provide faster processing than software-based encryption/decryption, the hardware-based approach may, in general, allow use of longer keys.

'193, Col. 201:50-62. There is no constraint placed on the "level of security desired" – it is up to the user or system designer (or someone – the patent does not say whom) to balance security

against their subjectively perceived costs in deciding what key lengths to use. The entire discussion of key lengths that follows is therefore dependent on a preference external to the patent. It is not enough to give technical details about key lengths, because whatever key length a person of skill in the art might choose or encounter fails to answer the question whether the product or activity in question is or isn't "secure" as used in the claims.

III. INTERTRUST'S EFFORTS TO DEFEND "SECURE" REVEAL THE INDEFINITE MEASURE OF SECURITY IMPLICIT IN THE PATENT

InterTrust's proposed solutions to the patent's lack of a standard for "secure" – its Markman definition and or a "commercially reasonability" standard – reveal precisely why the term is indefinite. The evidence confirms that "secure" as used in the claims has no fixed, precise meaning and is constrained by no criteria.

A. The Proposed Markman Definition Is Indefinite

Contrary to its concession of the need for criteria, InterTrust asserts that its proposed *Markman* definition of "secure" is sufficiently definite. InterTrust Opp., at 4. InterTrust's opposition brief omits, however, a crucial sentence within its proposed definition: "Security is not absolute, but designed to be sufficient for a particular purpose." Joint Claim Construction Statement, Exh. A, at 1. The definition states no "purpose," leaving the person of skill in the art completely in the dark as to how much security is needed, or for what, as well as how to measure it.

B. The Proposed Standard of "Commercial Reasonableness" Is Indefinite and Unsupported by the Patent

InterTrust's Opposition brief suggests an alternative definition for "secure" – "commercial reasonability." Having admitted the need for criteria, and challenged to show where the patents provide such criteria, InterTrust asserts that "[t]he information included in the InterTrust patents includes guidance regarding how security should be measured, including the statement that security should be based on a commercially reasonable standard." Opp., 3-4. Dr. Reiter elaborates in his declaration, reiterating the need for context and criteria, but stating that "computer security professionals routinely apply a commercial reasonability standard in building

security into real-world products and in determining whether real-world products or processes are 'secure.'" Reiter SJ Decl., at 12, 18.

If the "commercial reasonability" standard were in fact supported by the patent or the evidence, it would still leave the claims indefinite. But the Court need not even consider that question, because InterTrust's expert, Dr. Reiter, admits that the "commercially reasonable" standard referred to in his second Declaration differs from InterTrust's proposed *Markman* definition. When asked if he drafted the above-quoted sentence about computer security professionals "routinely apply[ing] a commercial reasonability standard," Dr. Reiter responded that he had neither drafted nor dictated it, saying only that he "remember[s] discussing issues like this with InterTrust before this was drafted, as far as I know, because I don't actually know when it was drafted." Reiter Depo., 4/17/03, p. 420:1-20 attached to Wesenberg Reply Decl., Exh. B. That led to the following exchange:

> Q: You recall discussing the opinion that computer security professionals routinely apply a commercial reasonability standard with InterTrust before you arrived at InterTrust and were given the draft of this declaration that's been marked as Exhibit 69?
>
> A. Certainly I remember discussing security is meant to be sufficient for a given purpose or a given set of threats and that requirements for commercial systems would be different than for other types of systems. I don't know if I used exactly the words commercial reasonability standard, though.
>
> Q. Do you understand "commercial reasonability standard" to be synonymous with "designed to be sufficient for a particular purpose"?
>
> A. I don't think I would say they're synonymous.
>
> Q. How do they differ?
>
> A. Commercial reasonability indicates a particular type of purpose or, you know, a particular – I should say maybe set of threats to which protection mechanisms should be robust or against which they should be robust.

Reiter Depo., 4/17/03, pp. 420:21-421:22, Wesenberg Reply Decl., Exh. B. "Commercial reasonability" thus not only means something different from InterTrust's proposed Markman definition, it also (unlike InterTrust's proposed Markman definition) gives at least a general indication what kinds of threats the system is to be secured against.

In fact, the commercial reasonability standard appears nowhere in the patent. Tellingly, Dr. Reiter's declaration does not assert that the patent teaches "commercial reasonability" – only InterTrust's brief makes that claim, citing two excerpts from the specification as support. InterTrust Opp., at 4 n.4. But the cited specification language says nothing about how to evaluate or define "reasonability." Rather, it refers to "sufficient security (sufficiently trusted) for the intended commercial purposes" and states that the level of security **depends on "the commercial requirements of particular markets or market niches, and may vary widely.**" '193, Col. 45:39-45, 49:59-62 (emphasis added). These statements effectively admit that "secure" is indefinite as used in the claims.

C. InterTrust Has Effectively Admitted that Secure Is Indefinite

The patent language that InterTrust cites as support for the "commercial reasonability" standard acknowledges that in these patents the only criteria of "secure" "depends on the commercial requirements of particular markets or market niches, and may vary widely." '193 patent, Col. 49:61-62, quoted in Joint Claim Construction Statement, Exh. C, item 19(B), 19(J), cited in InterTrust Opp., at 4 n.4. This admits indefiniteness, because no measure or method is identified which would let people of skill in the art precisely and reliably reach the same conclusion whether something is "secure" in those admittedly widely varying markets – especially where each of those markets consists of many different companies and people, and many possible different standards and "requirements."

InterTrust's brazenness in taking this position is apparently a function of its confidence that it can overwhelm Microsoft and the Court by citing to the numbing abundance of technical description in its gargantuan patents. The mere presence of voluminous description of possible technologies does not provide the needed measure.

IV. INTERTRUST COINED TERMS "PROTECTED PROCESSING ENVIRONMENT" AND "HOST PROCESSING ENVIRONMENT" AS USED IN ITS PATENTS LACK THE NECESSARY DEFINITENESS TO ONE OF ORDINARY SKILL IN THE ART

Like its arguments regarding "security," InterTrust's arguments regarding Protected Processing Environment ("PPE") and Host Processing Environment ("HPE") miss the

mark. In its Opposition, InterTrust simply ignores its burden of defining coined terms with "precision." *J.T. Eaton & Co. v. Atlantic Paste & Glue Co.*, 106 F. 3d 1563, 1570 (Fed. Cir. 1997). Instead it argues that HPE and PPE receive "extensive discussion in the specification."

Whatever the extent of the discussion, InterTrust points to no instance where these terms are clearly and ***precisely*** defined. Microsoft's primary contention is that when used, the coined phrases HPE or PPE, are used inconsistently, sometimes contradictorily and nearly always shrouded in qualifying and conditional language. The passages from the '193 specification attached to Dr. Reiter's declaration illustrate these defects. First, the nature of, and relationship between, "SPE", "PPE" and "HPE", is indeterminate. In a passage from the '193 specifications and cited by InterTrust's expert, the following relationship is described:

> ROS 602 in this example also includes one or more Host Event Processing Environment ("HPEs") 655 and/or one or more Secure Event Processing Environments ("SPEs") 503 (these environments may be generically referred to as "Protected Processing Environments" 650). (Col. 79, 30-35)

It can be surmised from this that reference to a PPE could mean either SPE or HPE. The specification, however, identifies that "HPEs" may be provided in two types, "Secure" and "Not Secure," and InterTrust leaves one to guess which is which in any given instance. Indeed, InterTrust admits that its proposed definition of HPE does not acknowledge this schism, yet InterTrust offers only a circularity as a remedy: that non-secure HPEs be defined to be HPEs that are not secure.

Any attempt to distinguish these terms by their structural or functional characteristics is futile. When text is actually committed to discussing a "PPE", "SPE" or "HPE" the qualities and/or attribute assigned each are merely optional. In the text following the introduction of the terms PPE and HPE (Col. 79, 31-35) the specification identifies no fewer than four attributes that "may" be aspects of an SPE or HPE. "HPEs and SPEs are self-contained computing and processing environments that ***may include*** their own operating system kernel, ... ***may process*** information in a secure way, ... they ***may*** each perform ... they ***may*** each offer ...". Reiter Decl., Ex. G., p. 2 (Col. 79, 36-46). (Emphasis added.) As demonstrated in this example, representations about functional and design characteristics of HPE's and PPE's are frequently

qualified with the term "may be" or "can be." The first two full paragraphs of Reiter Ex. G at p. 3 when referring to HPEs or SPEs use "may," "may be," "can be" or "could" fifteen times. Every sentence but one does so. The constant use of such qualifying language leaves one irredeemably confused as to the nature and characteristics of the PPEs and HPEs. Again, there is plenty of verbiage directed generally at these terms but they remain undefined, and certainly cannot be understood with anything approximating "precision."

InterTrust's argument that Professor Mitchell "has no difficulty understanding what the term [PPE] means" is both wrong and of no consequence. Microsoft has never disputed that one of ordinary skill in the art would be able to surmise what these coined terms ***might*** suggest when dissected into their component parts. The section of the Mitchell declaration cited by InterTrust is under the caption "what the claim appears to promise." This standard neither purports to, and does not, comport with the requirement of 35 U.S.C. § 112(2).

V. ARGUMENT

A. The Lack of Criteria or Parameters for "Secure" Render It Indefinite

InterTrust's concession that persons of skill in the art require criteria to understand "secure" with any precision, and that there are many different possible sets of criteria, greatly simplifies the analysis in this case. In *Amgen v. Hoechst Marion Roussel, Inc.*, the Federal Circuit held that claim language that could be measured by multiple recognized standards failed for indefiniteness where the written disclosure named several standards but failed to specify which one was to be used. 314 F.3d 1313, 1341-42 (Fed. Cir. 2003). Different methods of purifying human urinary erythropoietin ("uEPO") would produce samples with different glycosylation, which meant that the claim limitation "having glycosylation which differs from that of human uEPO" was a "'moving target.'" *Id.* at 1340, 1341 (quoting lower court). Finding that the specification of the patent "does not direct those of ordinary skill in the art to a standard by which the appropriate comparison can be made," the Court held that "such ambiguity in claim scope is at the heart of the definiteness requirement of 35 U.S.C. § 112 ¶ 2," and affirmed the lower court's finding of indefiniteness. *Id.*, at 1341, 1342. Similarly, the failure of the InterTrust patents to choose from among the many different standards by which "secure" could be

measured, or to specify clear criteria of its own, renders the claims containing the term "secure" and its variants indefinite.

B. <u>Indexing a Claim Term to Market Conditions Creates Impermissible Indefiniteness</u>

Instead of providing a standard, InterTrust has adopted the position that "secure" in this patent "depends on the commercial requirements of different markets or market niches, and may vary widely." That 'criterion' is an unpredictable, moving target, much like the claim term in *Ex parte Brummer*, 12 U.S.P.Q.2d 1653 (B.P.A.I. May 11, 1989). The term at issue in that case depended not on any objectively ascertainable feature, but on the label the manufacturer chose to place on the bicycle reflecting its subjective conception of the customer for whom the product was intended. *Id.*, at 1655. InterTrust's argument that this case is more like *Orthokinetics v. Safety Travel Chairs, Inc.*, 806 F.2d 1565 (Fed. Cir. 1986) is fallacious. In *Orthokinetics*, the term that depended on a factor outside the patent was a length parameter – a one-dimensional variable, so to speak. More importantly, it was not subjective. One of ordinary skill in the art building the claimed travel chair "would easily have been able to determine the appropriate dimensions" by measuring the particular automobile. *Id.* at 1576. The Court therefore found it unnecessary to require the claims to list "all possible lengths corresponding to the spaces in hundreds of different automobiles." *Id.* In *Brummer*, no amount of "listing" in the patent could possibly do the trick, because the terms on which the claim scope depended were subjective – the manufacturer's view of whom the bicycle was intended for, and the characteristics of the rider. Similarly, in this case, a person of skill in the art cannot possibly know what a particular customer, market or market niche will deem sufficiently "secure" until after it has sold the product.

Indeed, the fact that one cannot determine the scope of a claim until a product is first manufactured and sold demonstrates that the terms employing "secure" are also indefinite under the principle of *STX, Inc. v. Brine, Inc.*, 37 F. Supp. 2d 740 (D. Md. 1999), *aff'd* on other grounds, 211 F.3d 588 (Fed. Cir. 2000). In that case, subjective claim language describing a lacrosse stick ("improved handling and playing characteristics") would require one to play with

the stick in order to determine whether it possessed the limitation and therefore infringed. "The notion that one reasonably skilled in the art would have to infringe the patent claim in order to discern *the boundaries of the claim* is repugnant to long-standing principles of patent jurisprudence." *Id.*, at 755. Here too, one would have to manufacture and sell the product to determine whether it would enjoy market success and would thus have "sufficient security for the intended commercial purposes."

C. "Secure" Must Be Definite Because It Is Essential to VDE

InterTrust assails Microsoft for taking the position that the central importance of "secure" to VDE renders it crucial that the term be sufficiently definite. InterTrust Opp., at 20-21. Contrary to InterTrust's argument, Microsoft did not assert a lower standard of proof of indefiniteness; it sought to foreclose any such argument that InterTrust might make. InterTrust's own reading of *Exxon* confirms that noncritical limitations can sometimes be expressed in functional terms, while critical limitations cannot. Moreover, InterTrust's denial that its expert testified that security is "essential to VDE" is false. InterTrust Opp., at 21-22. Asked about "security," Dr. Reiter answered as follows: "I believe it's an essential aspect of VDE as described in the specification, or in the sense that certainly the authors invest a lot of time on questions of security, and so I think that's probably what they had in mind." Wesenberg Reply Decl., Exh. D (Reiter Depo., 2/28/03, at 23:16-20).[3] "Security" is a critical limitation, and must be sufficiently definite.

D. The Use of "Secure" in Other Patents (and Other Contexts) Is Completely Irrelevant to Whether the Claims at Issue Are Definite

It is a well-known aspect of indefiniteness case law that the same terms are held indefinite in some cases, and definite in others. Thus, the question of whether secure may have been used with sufficient definiteness in other patents, articles, etc., is irrelevant to whether it is sufficiently definite here. In holding that a claim using the term "about" was indefinite, the Federal Circuit warned: "In arriving at this conclusion, we caution that our holding that the term

---

[3] Microsoft's citation of this statement was off by five lines in the opening brief, the citation starting at line 21 instead of line 16 on the same page.

'about' renders indefinite claims 4 and 6 should not be understood as ruling out any and all uses of this term in patent claims. It may be acceptable in appropriate fact situations, even though it is not here." *Amgen, Inc. v. Chugai Pharmaceutical Co., Ltd.*, 927 F.2d 1200, 1218 (Fed. Cir. 1991). Microsoft has never argued that "secure" cannot be used with sufficient definiteness, only that InterTrust's patents fail to do so. InterTrust's arguments about Microsoft's use of "secure" in its patents are irrelevant, as well as mistaken. (For example, the Slivka '671 patent asserted in this case stands in marked contrast to InterTrust's use of "secure" in the claims at issue on this motion, not least because the Slivka '671 patent sets forth a clear standard by which secure or not secure can be evaluated).

1. <u>The Non-Patent Documents that Employ the Term Are Not Required to Satisfy 35 U.S.C. § 112</u>

Equally irrelevant is InterTrust's argument that "secure" is used in myriad publications and other contexts without the specification of every parameter. Microsoft agrees that "secure" is used in the art in many different ways, some quite vague. That is precisely why it is necessary to specify what is meant when using the term in a patent claim. Patent claims must satisfy 35 U.S.C. § 112(2); the publications InterTrust cites need not. (It is worth noting, however, that the only Microsoft publication provided to the Court by InterTrust uses the Common Criteria to evaluate security – in telling contrast to InterTrust's pervasive failure to identify a definite standard or measure by which "secure" can be evaluated by one of skill in the art. *See* Reiter SJ Decl., Exh. J).

VI. <u>INTERTRUST'S EFFORT TO INCORPORATE BY REFERENCE WAS INEFFECTIVE</u>

Patent Office practice surrounding incorporation by reference attempts to balance 1) the need to provide the public a complete written description of the patent (*see, e.g.*, 35 U.S.C. § 112) with 2) "economy, amplification, or clarity of exposition" achieved by allowing lengthy references to be incorporated by reference into an application under certain circumstances. *Ex parte Schwarze*, 151 USPQ 426 (B.P.A.I. 1966); *see* MPEP § 608.01(p). To meet this balance, the Patent Office has directed that: "essential" material may only be incorporated by reference to

an issued U.S. Patent or a published U.S. Patent Application. On the other hand, "nonessential material" may be referred to in a variety of ways. *See* MPEP § 608.01(p). Whether material has been incorporated by reference is a question of law. *Advanced Display Sys., Inc. v. Kent State University*, 212 F.3d 1272, 1282 (Fed. Cir. 2000). InterTrust does not deny that the Big Book material is essential material. The '683, '721, and '861 patents all purport to incorporate the "big book" by reference to the unpublished patent application. For example, the '721 states, "This application is related to commonly assigned copending application Ser. No. 08/388,107 of Ginter et al. . . . We incorporate by reference, into this application, the entire disclosure of this prior-filed Ginter et al. patent application." (721: 1:7-16; cf. 683: 1:7-23; 861 1:7-11). At the time that the applications leading to the '683, '721, and '861 patents were allowed, InterTrust could have easily complied with the appropriate requirement yet chose not to. Here, the '107 application is the "referenced application." The '107 application, in fact, NEVER issued as a patent – so the examiner had no duty to substitute. It is the duty of the applicant to comply with the 112 requirements. *United Carbon Co. v. Binney & Smith Co.*, 317 U.S. 228 (1942). Accordingly, InterTrust should have either taken one of the two simple options that was open to it. It chose not to. Its effort to incorporation by reference was ineffective.

VII. <u>CONCLUSION</u>

For the reasons set forth above, in Microsoft's opening brief and supporting documents and any argument that may be provided at the hearing, Microsoft respectfully ask this Court to grant its motion and find the mini-*Markman* claims to be invalid.

Dated: April 21, 2003

WILLIAM L. ANTHONY
ERIC L. WESENBERG
KENNETH J. HALPERN
ORRICK, HERRINGTON & SUTCLIFFE LLP

Eric L. Wesenberg
Attorneys for Defendant and Counterclaimant
MICROSOFT CORPORATION

IN THE UNITED STATES DISTRICT COURT

FOR THE NORTHERN DISTRICT OF CALIFORNIA

INTERTRUST TECHNOLOGIES CORPORATION, a Delaware corporation,

Plaintiff,

v.

MICROSOFT CORPORATION, a Washington corporation,

Defendant.

AND COUNTER-ACTION.

No. C 01-1640 SBA

Consolidated with No. C 02-0647 SBA

ORDER DENYING MOTION FOR PARTIAL SUMMARY JUDGMENT AND CONSTRUING "MINI-MARKMAN" CLAIMS

[Docket No. 229]

Plaintiff's Counsel are directed to serve this order upon all other parties in this action.

This matter comes before the Court for two related proceedings. The first is a "mini-Markman" (limited claim construction) proceeding in which the Court shall construe thirty terms and phrases appearing in twelve claims selected by the parties from the numerous claims at issue in this action. The second is Microsoft's Motion for Summary Judgment that Certain "Mini-Markman" Claims Are Invalid for Indefiniteness (the "Indefiniteness Motion"). The Court held a claim construction hearing on June 11 and 12, 2003, and heard oral argument on the Indefiniteness Motion on June 12, 2003. Having read and considered the papers submitted, having considered the parties' arguments at the hearings, and being fully informed, the Court DENIES the Indefiniteness Motion and CONSTRUES the disputed terms and phrases as set forth below.

United States District Court
For the Northern District of California

I. BACKGROUND

A. Procedural History

Plaintiff and counterdefendant InterTrust Technologies Corp. ("InterTrust") filed its Complaint in case number C 01-1640 SBA on April 26, 2001, its First Amended Complaint on June 26, 2001, its Second Amended Complaint on July 30, 2001, and its Third Amended Complaint on October 25, 2001. In its Third Amended Complaint InterTrust claimed infringement of seven patents. Defendant and counterclaimant Microsoft Corp. ("Microsoft") filed an answer and counterclaims to the Third Amended Complaint on November 15, 2001, alleging infringement of two of its own patents. The Court subsequently held one of the patents asserted in the Third Amended Complaint not infringed, leaving six patents-in-suit from the Third Amended Complaint.

On February 6, 2002, InterTrust filed a second, separate patent infringement action against Microsoft, No. C 02-0647 SBA, claiming infringement of an additional patent. That second patent infringement action was consolidated with the earlier-commenced action on May 3, 2002.

In an Order filed on October 23, 2002, the Court, inter alia, granted InterTrust leave to amend its complaint. Accordingly, on October 24, 2002, InterTrust filed its Fourth Amended Complaint, claiming infringement of eleven patents (i.e., it added infringement claims regarding four new patents), one of which was the patent-in-suit in Case No. C 02-0647 SBA. Per the Court's October 23, 2002 Order, Case No. C 02-0647 SBA was automatically dismissed as moot upon the filing of the Fourth Amended Complaint. In an Order filed on November 1, 2002, the Court stayed this action in part, staying all proceedings (including discovery) unrelated to twelve claims selected by the parties and listed in the Order; these claims would be subject to limited Markman and indefiniteness proceedings. On November 7, 2002, Microsoft filed an Answer and Counterclaims to InterTrust's Fourth Amended Complaint, in which it claimed infringement of the same two of its own patents that it had asserted in its previous answer and counterclaims.

Thus, at present, InterTrust has asserted eleven patents that are currently in suit, and Microsoft has asserted two, for a total of thirteen patents-in-suit. These patents are:

InterTrust:	5,892,900	(the "'900 patent")
	5,915,019	(the "'019 patent")
	5,917,912	(the "'912 patent")

	5,920,861	(the "'861 patent")
	5,949,876	(the "'876 patent")
	5,982,891	(the "'891 patent")
	6,112,181	(the "'181 patent")
	6,157,721	(the "'721 patent")
	6,185,683 B1	(the "'683 patent")
	6,253,193 B1	(the "'193 patent")
	6,389,402 B1	(the "'402 patent")
Microsoft:	6,049,671	(the "'671 patent")
	6,256,668	(the "'668 patent")

Both parties have asserted various affirmative defenses to the opposing party's infringement claims, and Microsoft additionally seeks declaratory judgments of non-infringement of InterTrust's asserted patents.

B. The Instant Proceedings

1. Mini-Markman Proceeding

Per the Court's Order of February 24, 2003, and the Court's relevant prior and subsequent Orders, the parties are before the Court for a "mini-Markman" proceeding. The Court is construing thirty terms and phrases from twelve claims jointly selected by the parties from the eleven patents asserted by InterTrust. The parties have asked for one additional item of construction: whether a particular term, "virtual distribution environment," should be read into all of the claims at issue as a limitation.[1] The terms and phrases to be construed have been selected from the following twelve claims (from seven of InterTrust's asserted patents):

1. 193.1[2]
2. 193.11
3. 193.15
4. 193.19
5. 683.2
6. 721.1
7. 721.34
8. 861.58
9. 891.1
10. 900.155
11. 912.8

---

[1] As discussed infra, there is some disagreement about whether Microsoft is asserting that this term should be read into every claim at issue in this proceeding.

[2] The format "XXX.YYY" indicates the following: XXX is the patent number; YYY is the number of the relevant claim in that patent. This format will be used to identify claims throughout this Order.

12. 912.35

The parties have filed a Patent Local Rule 4-3 Joint Claim Construction and Prehearing Statement Revised in Accordance with the Scope of "Mini-Markman" Hearing Set Forth in the Court's Order Entered 2/24/03 (the "JCCS"), which provides most of the essential information for the Court's construction of the terms and phrases at issue. The parties' competing proposed constructions of the terms and phrases are set out in Exhibits A and B to the JCCS (both exhibits provide the parties' proposed constructions but organize them differently). InterTrust's and Microsoft's identifications of intrinsic and extrinsic evidence are set out in Exhibits C and D, respectively, to the JCCS.

In connection with the mini-Markman hearing the parties have submitted the following briefs: InterTrust has submitted InterTrust's Opening Claim Construction Brief ("InterTrust's Opening Markman Brief") (40 pages in length); Microsoft has submitted Microsoft's Markman Brief (40 pages); and InterTrust has submitted Plaintiff InterTrust Technologies Corporation's Reply Memorandum on Claim Construction ("InterTrust's Reply Markman Brief") (25 pages). The parties have also submitted various declarations with attachments in support of their briefs. On InterTrust's motion, the Court struck the testimony of witnesses David Maier, Sanford Bingham, and Martin Plaehn, offered by Microsoft in support of its claim construction positions, in two Orders filed on June 5 and 10, 2003.

The parties have filed a Joint Appendix to Joint Claim Construction Statement (the "JA"), which consists of a brief cover document and 18 volumes containing the full seven patents-in-suit from which the 12 claims that are the subject of the mini-Markman proceeding are taken (Exhibits A through G), the prosecution histories of these seven patents (Exhibits H through Q), selected cited references (Exhibits R through DD), and a related patent application (Exhibit EE).

2. **Indefiniteness Motion**

Also per the Court's Order of February 24, 2003, and the Court's relevant prior and subsequent Orders, the parties are before the Court for resolution of Microsoft's Indefiniteness Motion. The Indefiniteness Motion seeks summary judgment on the issue that those of the claims at issue that contain any of the terms "secure," "protected processing environment," or "host

processing environment" are invalid as indefinite. These terms are three of the 30 terms to be construed in the mini-Markman proceeding.

The parties' briefing on the Indefiniteness Motion consists of the following: Microsoft's Brief in Support of Motion for Summary Judgment that Certain "Mini-Markman" Claims Are Invalid for Indefiniteness ("Microsoft's Opening Indefiniteness Brief"); the Memorandum of Points and Authorities of Plaintiff InterTrust Technologies in Opposition to Microsoft (sic) Motion for Summary Judgment on Indefiniteness and in Support of Cross-Motion for Summary Judgment ("InterTrust's Indefiniteness Opposition Brief");[3] and Reply to InterTrust's Opposition to Microsoft's Brief in Support of Motion for Summary Judgment that Certain "Mini-Markman" Claims Are Invalid for Indefiniteness" ("Microsoft's Reply Indefiniteness Brief"). Both parties' briefs overwhelmingly focus on the term "secure." The parties have also submitted various declarations with attachments in support of their briefs. Of Microsoft's evidentiary submissions, on InterTrust' motion the Court struck the testimony of witnesses Jim McLaughlin, Julien Signes, Damian Saccocio, and Karl Ginter,[4] in an Order filed on June 5, 2003.

II. LEGAL STANDARDS

A. Claim Construction Generally

A patent confers the right to exclude others from making, using, or selling the invention defined by the patent's claims. See Standard Oil Co. v. Am. Cyanamid Co., 774 F.2d 448, 452 (Fed. Cir. 1985). A patent must describe the exact scope of an invention and its manufacture to secure to a patentee all to which he is entitled, and to apprise the public of what is still open to them. See Markman v. Westview Instruments, Inc., 517 U.S. 370, 373, 116 S. Ct. 1384 (1996). These objectives are served by two distinct elements of a patent document. First, it contains a specification

[3] In filing its opposition brief to the Indefiniteness Motion, InterTrust asserted a Cross-motion for Partial Summary Judgment in which InterTrust sought summary judgment on the issue that eleven of the patent claims asserted by InterTrust are definite. In its Order Staying Cross-Motion and Briefing Thereon, filed on April 23, 2003, the Court stayed this cross-motion and all briefing related to the cross-motion until further order of the Court.

[4] Transcripts of these witnesses' testimony are appended to the Declaration of Eric L. Wesenberg in Support of Microsoft Corporation's Motion for Summary Judgment that Certain Mini-Markman Claims Are Indefinite as Exhibits C, D, H, and I, respectively.

United States District Court
For the Northern District of California

describing the invention in such full, clear, concise, and exact terms as to enable any person skilled in the art to make and use the same. See 35 U.S.C. § 112. Second, a patent includes one or more claims, which particularly point out and distinctly claim the subject matter which the applicant regards as his or her invention. See id.

The first step in any invalidity or infringement analysis is claim construction. See Union Oil Co. v. Atl. Richfield Co., 208 F.3d 989, 995 (Fed. Cir. 2000). The construction of claims is simply a way of elaborating the normally terse claim language in order to understand and explain, but not to change, the scope of the claims. See id. Claim construction is a matter of law to be determined by the court. See Markman v. Westview Instruments, Inc., 52 F.3d 967, 979 (Fed. Cir. 1995), aff'd, 517 U.S. 370, 116 S.Ct. 1384 (1996).

B. Consideration of Evidence in Connection with Claim Construction

1. Intrinsic Evidence

"It is well-settled that, in interpreting an asserted claim, the court should look first to the intrinsic evidence of record, i.e., the patent itself, including the claims, the specification, and, if in evidence, the prosecution history." Vitronics Corp. v. Conceptronic, Inc., 90 F.3d 1576, 1582 (Fed. Cir. 1996) (citing Markman, 52 F.3d at 979). In the context of the intrinsic evidence, the court should first look to the language of the claims themselves. See id. Words in a claim are generally given their ordinary and customary meaning as understood by one of ordinary skill in the art. See id.; see also Dow Chem. Co. v. Sumitoro Chem. Co., 257 F.3d 1364, 1373 (Fed. Cir. 2001) ("[A] technical term used in a patent claim is interpreted as having the meaning a person of ordinary skill in the field of invention would understand it to mean."). It is well-established that "dictionaries, encyclopedias and treatises are particularly useful resources to assist the court in determining the ordinary and customary meanings of claim terms." Tex. Digital Sys., Inc. v. Telegenix, Inc., 305 F.3d 1193, 1202 (Fed. Cir. 2002); see also Dow Chem., 257 F.3d at 1373 ("Dictionaries and technical treatises . . . hold a special place and may sometimes be considered along with the intrinsic

evidence when determining the ordinary meaning of claim terms.").[5] A dictionary definition may not be relied on, however, if it contradicts any definition found in or ascertained by a reading of the patent documents. See Kopykake Enters., Inc. v. Lucks Co., 264 F.3d 1377, 1382 (Fed. Cir. 2001) (citing Vitronics, 90 F.3d at 1584 n.6). The Court should rely on specialized, technical dictionaries that reflect the understanding of one skilled in the art, rather than lay dictionaries. AFG Indus. v. Cardinal, 239 F.3d 1239, 1247–48 (Fed. Cir. 2001) ("Dictionary definitions of ordinary words are rarely dispositive of their meanings in a technological context.") (citing Anderson v. Int'l Eng'g & Mfg., Inc., 160 F.3d 1345, 1348–49 (Fed. Cir. 1998); see also Hoescht Celanese Corp. v. BP Chems. Ltd., 78 F.3d 1575, 1580 (Fed. Cir. 1996)).

"Although words in a claim are generally given their ordinary and customary meaning, a patentee may choose to be his own lexicographer and use terms in a manner other than their ordinary meaning, provided the special definition of the term is clearly stated in the specification." Vitronics, 90 F.3d at 1582. Therefore, it is necessary to review the specification to determine whether the patentee has used terms inconsistent with their ordinary and customary meaning. See id.; see also Dow Chem., 257 F.3d at 1373 ("[T]he court must examine the intrinsic evidence to determine whether the patentee has given a term an unconventional meaning."). Thus, the specification acts as a dictionary when it expressly defines a term used in the claim or defines it by implication. See Vitronics, 90 F.3d at 1582 (citing Markman, 52 F.3d at 979). However, in examining the specification, the court must not read limitations from the specification into the claims. See Burke, Inc. v. Bruno Indep. Living Aids, Inc., 183 F.3d 1334, 1340 (Fed Cir. 1999); Comark Communications, Inc. v. Harris Corp., 145 F.3d 1182, 1186–87 (Fed. Cir. 1998) (limitations from specification are not to be read into the claims, but there is a fine line between reading a claim in light of the specification and reading a limitation into the claim from the specification); but see Scimed Life Sys., Inc. v. Advanced Cardiovascular Sys., 242 F.3d 1337, 1341 (Fed. Cir. 2001)

---

[5] Although such materials have regularly been characterized as extrinsic evidence, albeit special extrinsic evidence that may be considered along with intrinsic evidence, e.g., Dow Chem., 257 F.3d at 1373, the Federal Circuit has cautioned that "categorizing them as 'extrinsic evidence' or even a 'special form of extrinsic evidence' is misplaced and does not inform the analysis." Tex. Digital, 305 F.3d at 1203.

("Where the specification makes clear that the invention does not include a particular feature, that feature is deemed to be outside the reach of the claims of the patent, even though the language of the claims, read without reference to the specification, might be considered broad enough to encompass the feature in question.").

Finally, if it is entered into evidence, the court must examine the prosecution history of the patent. See Dow Chem., 257 F.3d at 1373; Vitronics, 90 F.3d at 1582. The prosecution history contains the complete record of the proceedings before the Patent and Trademark Office, and may include express representations made by the applicant regarding the scope of the claims. See Vitronics, 90 F.3d at 1582. The court examines the prosecution history to determine "whether the patentee has 'relinquished a potential claim construction in an amendment to the claim or in an argument to overcome or distinguish a reference.'" Dow Chem., 257 F.3d at 1373 (citing Interactive Gift Exp., Inc. v. Compuserve Inc., 256 F.3d 1323, 1331 (Fed. Cir. 2001)); see also Pall Corp. v. PTI Technologies Inc., 259 F.3d 1383, 1392 (Fed. Cir. 2001) ("[I]t is well established that '[t]he prosecution history limits the interpretation of claim terms so as to exclude any interpretation that was disclaimed during prosecution.'") (citing Southwall Technologies, Inc. v. Cardinal IG Co., 54 F.3d 1570, 1576 (Fed. Cir. 1995)). A narrower claim interpretation will be adopted if the "accused infringer can demonstrate that the patentee 'defined' the claim as 'excluding' a broader interpretation 'with reasonable clarity and deliberateness.'" Pall Corp., 259 F.3d at 1393 (citing N. Telecom Ltd. v. Samsung Elecs. Co., 215 F.3d 1281, 1294–95 (Fed. Cir. 2000)).

2. Extrinsic Evidence

In most cases, an examination of the intrinsic evidence will be sufficient to resolve any ambiguity in the disputed claim and it would be improper to rely on extrinsic evidence. See Vitronics, 90 F.3d at 1583 (citing Pall Corp. v. Micron Separations, Inc., 66 F.3d 1211, 1216 (Fed. Cir. 1995)). Extrinsic evidence may be used to define the claim only if the claim language remains "genuinely ambiguous" after consideration of the intrinsic evidence. See id. However, "it is entirely appropriate, perhaps even preferable, for a court to consult trustworthy extrinsic evidence to ensure that the claim constructions it is tending to from the patent file is not inconsistent with clearly expressed, plainly apposite, and widely held understandings in the pertinent technical field.'" AFG

Indus., 239 F.3d at 1249 (quoting Pitney Bowes, Inc. v. Hewlett-Packard Co., 182 F.3d 1298, 1309 (Fed. Cir. 1999)); see also Bell v. Howell Document Mgmt. Prods. Co., 132 F.3d 701, 706 (Fed. Cir. 1998); Mantech Envtl. Corp. v. Hudson Envtl. Servs., Inc., 152 F.3d 1368, 1373 (Fed. Cir. 1998).

> When "the specification explains and defines a term used in the claims, without ambiguity or incompleteness, there is no need to search further for the meaning of the term." However, when such definition is challenged it is often appropriate, despite facial clarity and sufficiency of the specification and the prosecution history, to receive evidence of the meaning and usage of terms of art from persons experienced in the field of the invention.

ATD Corp. v. Lydall, Inc., 159 F.3d 534, 540 (Fed. Cir. 1998) (citations omitted). A court may hear all relevant testimony—including expert testimony—so long as it does not accord weight to expert testimony that contradicts the clear language of the claim. See Vitronics, 90 F.3d at 1584.

C. Invalidity Based on Indefiniteness

A patent is presumed to be valid. 35 U.S.C. § 282. A party challenging the validity of a patent must prove the invalidity by clear and convincing evidence. See Apotex USA, Inc. v. Merck & Co., 254 F.3d 1031, 1036 (Fed. Cir. 2001); Loral Fairchild Corp. v. Matsushita Elec. Indus. Co., 266 F.3d 1358, 1361 (Fed. Cir. 2001).

A patent claim satisfies the definiteness requirement of paragraph 2 of 35 U.S.C. § 112 only if "one skilled in the art would understand the bounds of the claim when read in light of the specification." Exxon Research & Eng'g Co. v. United States, 265 F.3d 1371, 1375 (Fed. Cir. 2001) (citing Miles Labs., Inc. v. Shandon, Inc., 997 F.2d 870, 875 (Fed. Cir. 1993)). This means that the claims at issue must be "sufficiently precise to permit a potential competitor to determine whether or not he is infringing." Morton Int'l, Inc. v. Cardinal Chem. Co., 5 F.3d 1464, 1470 (Fed. Cir. 1993). But a claim is not indefinite "merely because it poses a difficult issue of claim construction"; the claim need only "be amenable to construction, however difficult that task may be." Exxon Research, 265 F.3d at 1375. Whether a claim is indefinite is a question of law. Id. at 1376.[6]

---

[6] In Microsoft's Opening Indefiniteness Brief, Microsoft claims that the determination of definiteness involves application of a two-part test. (Microsoft's Opening Indefiniteness Br. at 21.) InterTrust disputes the validity of this test, arguing that the Federal Circuit has clearly rejected the requirement, asserted by Microsoft, that claims be drafted as precisely or specifically as possible. (InterTrust's Indefiniteness Opp. Br. at 15 (quoting PPG Indus., Inc. v. Guardian Indus. Corp., 156 F.3d

<u>III. DISCUSSION</u>

As an initial matter, the Court notes that the relevant "art" of the claims at issue in the mini-Markman proceeding and the Indefiniteness Motion is computer security. The Court previously reached this conclusion in its Order re: Unresolved Portion of InterTrust's Motion to Strike Markman Matter after considering supplemental briefing on this issue, and the Court now incorporates by reference its reasoning therein.[7]

The Court addresses the Indefiniteness Motion first for a practical reason: if any of the terms at issue are found indefinite, there would be no need to construe any claim that contains such term or terms.

A. <u>Indefiniteness Motion</u>

Microsoft's Indefiniteness Motion seeks summary judgment on the issue of whether the claims at issue are indefinite with regard to three terms: "secure"; "protected processing environment"; and "host processing environment." The overwhelming majority of the briefing, however, is addressed solely to the term secure. These terms are discussed in turn.

1. <u>Secure</u>

Although Microsoft's discussion of why the term secure is indefinite is lengthy both in its opening brief and its reply brief, the essence of its theory of indefiniteness is a ten-variable test created by Microsoft's expert, Professor John C. Mitchell ("Prof. Mitchell"), which, he contends, is

---

1351, 1355 (Fed. Cir. 1998), and Exxon Research, 265 F.3d at 1376, 1383–84).)

The Court agrees with InterTrust that Microsoft's asserted two-part test has no basis in law. The principles set forth above in this section of the Order are what govern consideration of Microsoft's Indefiniteness Motion. Microsoft's counsel was prudent to retreat from this alleged two-part test at oral argument, (see Transcript of Proceedings, Claims Construction Hearing ("Tr.") 305:24–306:13), although Microsoft should not have advanced it in the first place.

[7] The Court needs not and does not define what experience or qualifications one must have to be a "person of ordinary skill in the art" of computer security. The Court already struck the testimony of certain of Microsoft's witnesses in its Order re: InterTrust's Motions to Strike on the ground that there was insufficient evidence that they had sufficient skill even under Microsoft's lenient standard of "ordinary skill." None of the remaining testimony tendered by the parties would be subject to exclusion on the ground that the declarant lacked sufficient skill to be competent to testify. Thus, the Court concludes that all remaining witnesses providing testimony regarding the proper construction of the terms and phrases in dispute, particularly Dr. Michael Reiter and Professor John C. Mitchell, have at least the ordinary skill in the art, and the Court evaluates the evidence accordingly.

not satisfied with respect to secure. Specifically, Prof. Mitchell asserts that in order for persons of ordinary skill in the art to understand what is meant by the term secure, they must be able to reach a common understanding with regard to each of the following variables:

1. Protecting what types of things or actions?
2. Protecting what specific things or actions?
3. Protecting what properties of these things or actions (e.g., secrecy/confidentiality, integrity, availability, authenticity, and non-repudiation)?
4. Protecting against whom?
5. Protecting against what points of attack?
6. Protecting against what kind of attacks?
7. Secure for how long?
8. How to test or infer the existence of the protection?
9. What degree of protection?
10. Secure to whom?

(Decl. of Professor John C. Mitchell at 9–11.) Prof. Mitchell's Declaration presents numerous excerpts from the relevant specifications that, he evidently believes, do not allow persons of ordinary skill in the art to reach common understandings regarding any or all of these variables. (See, e.g., id. at 12–18.) Given that the Court has stricken the testimony of witnesses Signes, McLaughlin, Saccocio, and Ginter, Prof. Mitchell's testimony constitutes virtually the entirety of the evidentiary support, other than the text of the claims and specifications themselves, for Microsoft's positions in the Indefiniteness Motion.

InterTrust advances a number of arguments in response to Microsoft's contentions. First, it points out that Prof. Mitchell testified that secure has a general meaning in the field of computer science, and he himself was able to explain his use of the word secure. (InterTrust's Indefiniteness Opp. Br. at 4.) Prof. Mitchell also testified that there is a recognized set of criteria for determining whether a system is secure. (Id. at 5.) Second, InterTrust asserts that the claims of the patents-in-suit use secure in context, placing qualifiers around it that make clear to what they are referring. (Id. at 5–7.) Third, InterTrust notes that Prof. Mitchell's ten-variable test was created for the purposes of litigation and that Prof. Mitchell does not apply this test to any other document; indeed, as InterTrust's expert, Dr. Michael Reiter ("Dr. Reiter"), testifies, Microsoft's own patents and Prof. Mitchell's own computer security papers fail the test. (Id. at 8.) Relatedly, InterTrust provides various examples in which Prof. Mitchell appears to understand what secure means in context, yet he nevertheless finds the term indefinite because it fails to meet his ten-variable test. (Id. at 8–9.)

Fourth, InterTrust, emphasizing that Microsoft must produce clear and convincing evidence, describes the relevant standard for determining indefiniteness, noting that the use of general terms to describe a range of circumstances does not render claims indefinite and that the fact that reasonable persons might disagree regarding the scope of claims does not render them indefinite. (Id. at 10–14.) InterTrust adds that Microsoft's assertion that 35 U.S.C. § 112 requires claims to be drafted "as precisely or specifically as possible" to be definite has been expressly rejected by the Federal Circuit in PPG Industries, Inc. v. Guardian Industries Corp., 156 F.3d 1351 (Fed. Cir. 1998). (Id. at 15.) Fifth, InterTrust notes that the terms secure and securely are used in other patents, including Microsoft's patents. (Id. at 17.) Sixth, InterTrust explains that the Patent and Trademark Office ("PTO") examiners assigned to the InterTrust applications had no difficulty applying the disputed terms to the prior art. (Id. at 18.) Seventh, InterTrust contends that Prof. Mitchell's analysis should be discarded because he made no attempt to construe the claims as a whole, but rather focused on secure in isolation. (Id. at 18–19.) Eighth, InterTrust seeks to distinguish the cases offered by Microsoft in which certain claim terms were held indefinite on the basis that those cases concerned patent applications, not issued patents; in the former there is no presumption of validity, whereas there is such a presumption for the latter. (Id. at 20–22.)

In its reply brief, Microsoft addresses several of InterTrust's arguments. Of particular note is Microsoft's argument that certain patent language defines secure with reference to a particular purpose, but that purpose is not explicitly defined (e.g., commercial requirements), thereby leaving the reader in the dark about the scope of the claim. (Microsoft's Indefiniteness Reply Br. at 7–9, 11–12.) In particular, Microsoft argues that to the extent that secure is defined with reference to the context of the invention's commercial embodiments, it is indefinite. (Id. at 12–13.)[8] In addition,

---

[8] Related to but independent of the foregoing, Microsoft contends that the effort to incorporate by reference the "Big Book" patent application filed in or about 1995 with respect to the '683, '721, and '861 patents failed because these patents reference the number of the Big Book application, which did not result in an issued patent and therefore was not published. (See Microsoft's Indefiniteness Opening Br. at 12; Microsoft's Indefiniteness Reply Br. at 14–15.) Microsoft contends that "essential" material such as this may be incorporated in a patent only by reference to an issued U.S. Patent or a published U.S. Patent Application. (Microsoft's Indefiniteness Opening Br. at 12.) Microsoft appears to be relying exclusively on § 608.01(p) of the Manual of Patent Examining Procedure (the "MPEP"). (Id.)

Microsoft, quoting deposition testimony of Prof. Mitchell, disputes InterTrust's contention that Prof. Mitchell did not attempt to understand claim terms in the context of the claims. (Id. at 3–4.)

At first blush, Microsoft's arguments and examples are appealing: when read in isolation, many of the claims' uses of the term secure superficially appear ambiguous. But InterTrust has made a convincing case that Microsoft's arguments must be rejected. Perhaps most crucially, the Court agrees with InterTrust that Prof. Mitchell's test is not credible. Prof. Mitchell's test is so unusual and unsupported—probably because, as he admitted, it was created for this litigation—that the Court finds it not credible. There is no evidence whatever, other than Prof. Mitchell's self-serving assertion, that a person of ordinary skill in the art would require definition of all ten variables in the test to understand what is meant by secure. Still further, Prof. Mitchell's opinions are suspect because his declaration does not reflect that he has made any effort to understand the meaning of secure in the context of the claims in their entirety, his deposition testimony on this point

---

InterTrust disagrees with Microsoft's argument about incorporation by reference. InterTrust contends that there was merely a clerical error. (InterTrust's Indefiniteness Opp. Br. at 23–24.) InterTrust continues that incorporation by reference is effective if the referenced material is reasonably available to the public, and because, according to the MPEP, pending or abandoned applications are readily available to the public from the Patent Office, the Big Book patent application was effectively incorporated. (Id. at 24–25.) InterTrust further argues that MPEP § 608.01(p) requires only that the examiner is supposed to replace an application number with the issued patent number; it does not hold that a patent does not successfully incorporate by reference the material in question if the examiner fails to do so. (Id. at 25.)

The Court finds Microsoft's argument unpersuasive. Microsoft has made no effort to explain how the MPEP constitutes binding authority. To the contrary, the Foreward of the MPEP, of which the Court takes judicial notice, describes the purpose of the MPEP in part as follows:

> This Manual is published to provide U.S. Patent and Trademark Office patent examiners, applicants, attorneys, agents, and representatives of applicants with a reference work on the practices and procedures relative to the prosecution of patent applications before the U.S. Patent and Trademark Office. It contains instructions to examiners, as well as other material in the nature of information and interpretation, and outlines the current procedures which the examiners are required or authorized to follow in appropriate cases in the normal examination of a patent application. The Manual does not have the force of law or the force of the rules in Title 37 of the Code of Federal Regulations.

United States Patent & Trademark Office, Manual of Patent Examining Procedure (Rev. 1, Feb. 2003), available at http://www.uspto.gov/web/offices/pac/mpep/mpep_e8r1_front.pdf (emphasis added). Moreover, the Court has reviewed MPEP § 608.01(p), and the Court agrees with InterTrust that that provision appears only to indicate that the patent examiner should replace an application number with the issued patent number. Accordingly, the Court cannot conclude that the error at issue has resulted in the nonincorporation of the Big Book application by reference.

notwithstanding. Such an approach is not consistent with proper claim construction, which requires interpretation of each claim as a whole. Prof. Mitchell's conspicuous failure to apply his test to the use of the word in other documents suggests that the test has been generated for selective application to InterTrust's patents. And even more damaging to the test's credibility is Dr. Reiter's testimony that application of this test to Microsoft's own patents renders them indefinite.[9] The need to satisfy this test thus seems more hypothetical than real.

Further, as InterTrust correctly points out, the mere fact that persons skilled in the art might disagree about the scope of the claims at issue does not render them indefinite. As the Federal Circuit has observed, "It may of course occur that persons experienced in a technologic field will have divergent opinions as to the meaning of a term, particularly as narrow distinctions are drawn by the parties or warranted by the technology. . . . But the fact that the parties disagree about claim scope does not of itself render the claim invalid." Verve, LLC v. Crane Cams, Inc., 311 F.2d 1116, 1120 (Fed. Cir. 2002).

Nor are the claims at issue indefinite because they use a term that requires an evaluation of the context in which it is used or describes a range of circumstances. On this score the Federal Circuit's reasoning and holding in Orthokinetics, Inc. v. Safety Travel Chairs, Inc., 806 F.2d 1565 (Fed. Cir. 1986), discussed by InterTrust in its opposition brief and at the hearing, demonstrate that Microsoft's concerns are overstated. In Orthokinetics, the Federal Circuit considered whether the term "so dimensioned" from the following claim language was indefinite: "In a wheel chair having a seat portion, a front leg portion, and a rear wheel assembly, the improvement wherein said front leg portion is so dimensioned as to be insertable through the space between the doorframe of an

---

[9] Microsoft does not respond in its reply brief to Dr. Reiter's testimony about how application of Prof. Mitchell's ten-variable test to several of Microsoft's own patents renders them indefinite. (Microsoft's counsel's assertion at oral argument that Microsoft did address this point in its reply brief, (Tr. 307:15–23), is inaccurate.) At oral argument, however, Microsoft's counsel sought to refute this testimony by arguing that the '671 patent (one of the two patents asserted by Microsoft) expressly defines something to be "secure" as when it is digitally signed. (Tr. 287:22–288:3.) Whatever the merits of this argument, it does not contradict Dr. Reiter's testimony that five other patents held by Microsoft would be indefinite if Prof. Mitchell's test were applied to them. (Decl. of Dr. Michael Reiter in Opp. to Indefiniteness Mot. and in Supp. of InterTrust's Cross-Motion for Summ. J. Ex. D, cited in InterTrust's Indefiniteness Opp. Br. at 8.) The significance of this testimony is that it undermines the credibility of Prof. Mitchell's ten-variable test as representing the perspective of a person of ordinary skill in the art of computer security.

automobile and one of the seats thereof . . . ." Id. at 1568 (emphasis added). The district court had concluded that "so dimensioned" was indefinite because a potential competitor would have to construct a model of a travel chair and test the model on a variety of automobiles before the competitor could determine whether it infringed the patent. See id. at 1575. The Federal Circuit reversed, reasoning:

> It is undisputed that the claims require that one desiring to build and use a travel chair must measure the space between the selected automobile's doorframe and its seat and then dimension the front legs of the travel chair so they will fit in that particular space in that particular automobile. Orthokinetics' witnesses, who were skilled in the art, testified that such a task is evident from the specification and that one of ordinary skill in the art would easily have been able to determine the appropriate dimensions. . . . [¶] That a particular chair on which the claims read may fit within some automobiles and not others is of no moment. The phrase "so dimensioned" is as accurate as the subject matter permits, automobiles being of various sizes. As long as those of ordinary skill in the art realized that the dimensions could be easily obtained, [35 U.S.C.] § 112, 2d ¶ requires nothing more. The patent law does not require that all possible lengths corresponding to the spaces in hundreds of different automobiles be listed in the patent, let alone that they be listed in the claims.

Id. at 1576 (citations omitted).

Similarly, Microsoft has failed to demonstrate that a person of ordinary skill in the art would be unable to determine from the language of the claims and the specifications whether a device might be secure in a sense contemplated by the claims at issue. For example, Microsoft, citing STX, Inc. v. Brine, Inc., 37 F. Supp. 2d 740 (D. Md. 1999), aff'd on other grounds, 211 F.3d 588 (Fed. Cir. 2000), contends that secure is indefinite to the extent that it is defined with reference to the commercial purpose for which it is intended to be used. (Microsoft's Indefiniteness Reply Br. at 12.) Microsoft argues that if one of ordinary skill in the art would have to infringe the patent claim to discern the boundaries of the claim, the claim must be indefinite. (Id. at 12–13.)

The Court agrees with the general proposition that Microsoft advances. But Microsoft, which bears a heavy burden to demonstrate indefiniteness, has failed to offer sufficient evidence that a person of ordinary skill in the art could not discern what would be considered "secure" for a given commercial purpose. Its unsupported assertion in its reply brief that "a person of skill in the art cannot possibly know what a particular customer, market or market niche will deem sufficiently 'secure' until after it has sold the product," (id. at 12), is no substitute for evidence to this effect. Nor is its effort to distinguish Orthokinetics availing: That Orthokinetics involved measurement of a

"one-dimensional variable," namely length, (see id.), does not demonstrate that persons of ordinary skill in the art of computer security cannot effectively "measure" several variables. In addition, the fact that "secure" is subjective, in contrast to the clearly objective variable of length, (see id.), does not mean that a person of ordinary skill in the art cannot determine whether or not something is secure within the context that the term is used. The Court is also unaware of any principle in patent law that all operative claim terms must be measurable by some objective standard, and Microsoft does not advance any authority in support of such principle. In sum, it is not self-evident that potential designers of computer security systems are incapable of accurately assessing the commercial purposes for which their systems would be utilized to determine whether these systems are secure within the meaning of the claims at issue and, therefore, whether they infringe them. In the absence of clear and convincing evidence that a person of ordinary skill in the art would be unable to perform this task successfully, the Court cannot conclude that the claims at issue are indefinite.

Were Microsoft not to bear the burden of proving indefiniteness by a clear-and-convincing evidentiary standard, resolution of the Indefiniteness Motion might present a closer call. But such is not the case here. There is no clear and convincing evidence that InterTrust's claims are invalid as indefinite to the extent they contain the term secure. The Court thus DENIES the Indefiniteness Motion with regard to the term secure.

2. Protected Processing Environment (PPE) and Host Processing Environment (HPE)

Microsoft contends that the terms protected processing environment ("PPE") and host processing environment ("HPE") do not have an ordinary or customary meaning inside or outside of the computing world. (Microsoft's Indefiniteness Opening Br. at 15.) Microsoft notes that InterTrust's expert Dr. Reiter testified that a person of ordinary skill in the art would not know what these terms meant in 1995. (Id. at 16.) Citing J.T. Eaton & Co. v. Atlantic Paste & Glue Co., 106 F.3d 1563, 1570 (Fed. Cir. 1997), Microsoft contends that because a person of ordinary skill in the art would not understand these terms, it was InterTrust's duty to supply a precise meaning for these terms. (Id. at 15; see also Microsoft's Indefiniteness Reply Br. at 10.) Microsoft asserts that neither

the claims nor the specification provides sufficient description of PPE or HPE to inform a person of ordinary skill in the art what these terms mean. (Microsoft's Indefiniteness Opening Br. at 16–19.)

InterTrust responds that, with regard to PPE, the specification provides detailed descriptions of the key terms on which PPE is based (i.e., secure processing environment ("SPE") and HPE), and therefore PPE is sufficiently defined. (See InterTrust's Indefiniteness Opp. Br. at 22.) InterTrust also points to the various figures in the specification, spread out over dozens of pages, that relate to PPE. (Id.) InterTrust further cites to the Declaration of Dr. Michael Reiter in Opposition to Microsoft's Motion for Summary Judgment and in Support of InterTrust's Cross-Motion for Summary Judgment (the "Reiter Indefiniteness Declaration"), which provides excerpts from the relevant specifications. (Id. (citing Reiter Indefiniteness Decl. ¶¶ 39–40, Ex. G).) Finally, InterTrust rejects Prof. Mitchell's finding PPE indefinite based on application of his ten-variable test. (Id.) As for HPE, InterTrust contends that Microsoft has disingenuously claimed an absence of description in the specification: InterTrust asserts that the terms host processing environment and HPE are used interchangeably; even though the term host processing environment does not frequently appear in the specification, HPE does, along with extensive descriptions. (Id. at 23.)

The potential indefiniteness of these two terms was not addressed at the mini-Markman hearing, but the Court is comfortable resolving the issue on the papers. At the outset, Microsoft's citation to J.T. Eaton & Co. v. Atlantic Paste & Glue Co., 106 F.3d 1563, 1570 (Fed. Cir. 1997), is inapposite. J.T. Eaton has nothing to do with invalidity for indefiniteness, and the cited portion describes merely the patent applicant's obligation to define a coined term precisely in prosecuting its application. See id. at 1568, 1570. Perhaps under J.T. Eaton InterTrust was required to define PPE and HPE when it was prosecuting its applications for the patents-in-suit, but the Federal Circuit's holding therein does not alter Microsoft's burden to provide clear and convincing evidence of indefiniteness.

Microsoft has failed to carry that burden with regard to PPE and HPE. Microsoft itself recognizes that PPE is described to be an SPE and/or an HPE. (Microsoft's Indefiniteness Opening

Br. at 19 (quoting '193 patent at 105:18–21).)[10] Contrary to Microsoft's assertion, this definition by reference is not inherently an unhelpful exercise; it is fruitless only if the incorporated terms are themselves indefinite. Since Microsoft does not contest the clarity or definiteness of SPE, the Court examines only the definiteness of HPE. The Court discusses the proper construction of HPE infra, but in the meantime, it is sufficient for the Court to conclude that Microsoft has failed to provide clear and convincing evidence of indefiniteness. Microsoft's evidence pertaining to HPE, aside from evidence that HPE did not have a meaning known by a person of ordinary skill in the art, consists essentially of a few references to the '900 patent specification. (Id.)[11] But the Court agrees with InterTrust that the description of HPEs in the portion of the '193 patent specification that it cites, ('193 patent at 79:23–83:9), as well as the various figures referenced therein, (e.g., '193 patent Fig. 10), provide sufficient meaning to the term HPE to survive an indefiniteness challenge.

Were InterTrust now applying for the relevant patents-in-suit, and were the Court the PTO, the Court might require InterTrust to provide greater precision in defining PPE and HPE. But the parties are now before the Court on Microsoft's challenge to the relevant claims' validity, and thus Microsoft bears a heavy burden if its motion is to succeed. In presenting its arguments regarding PPE and HPE, Microsoft appears inclined to shift the burden to InterTrust to defend the validity of its claims. But the burden remains with Microsoft, and Microsoft has failed to put forward sufficient evidence to carry its burden. Accordingly, the Court DENIES the Indefiniteness Motion with regard to the terms PPE and HPE.

///

///

///

---

[10] Microsoft evidently considers this definition problematic: "This [definition] invariably leaves the relevant public guessing at what might infringe." (Id.) The Court disagrees. Obviously, if PPE is defined to include both SPEs and HPEs, for any embodiment that includes an SPE and/or an HPE and that has other features on which the relevant claim limitations read, the relevant claim is infringed. Thus, for example, the element in 683.2 that provides in part, "a protected processing environment at least in part protecting information . . ." encompasses SPEs and/or HPEs; the public need not guess between SPEs and HPEs, because PPE is defined to include both.

[11] The Court previously struck the testimony of Envivio's and America Online's corporate designees, cited by Microsoft in its Indefiniteness Opening Brief.

United States District Court
For the Northern District of California

B. Construction of Claims at Issue

1. Terms and Phrases for Which Microsoft Did Not Brief Its Position

Out of the thirty terms and phrases selected by the parties for construction, Microsoft elected not to present any argument in its 40-page Markman brief in support of its positions or in opposition to InterTrust's positions on thirteen terms and phrases. These terms and phrases, along with the claims in which they appear, are:

1. aspect (683.2, 861.58, 900.155, 912.8)
2. authentication (193.15)
3. budget (193.1)
4. clearinghouse (193.19)
5. compares (900.155)
6. derive (900.155)
7. designating (721.1)
8. device class (721.1)
9. digital signature/digitally signing (721.1)
10. digitally signing a second load module with a second digital signature different from the first digital signature, the second digital signature designating the second load module for use by a second device class having at least one of tamper resistance and security level different from the at least one of tamper resistance and security level of the first device class (721.1)
11. executable programming/executable (721.34, 912.8, 912.35)
12. identifying at least one aspect of an execution space required for use and/or execution of the load module (912.8)
13. securely applying, at said first appliance through use of said at least one resource said first entity's control and said second entity's control to govern use of said data item (891.1)

At the mini-Markman hearing the Court stated its disinclination to hear oral argument regarding any of these thirteen terms and phrases. The Court reasonably concluded that Microsoft made a decision

not to dispute or oppose InterTrust's proposed constructions of these terms and phrases given (1) the number of terms Microsoft declined to address; (2) the importance of written argumentation for the mini-Markman proceeding; and (3) the fact that InterTrust did address every term and phrase at issue.[12]

The Court has reviewed all of InterTrust's briefing on these terms and phrases and finds InterTrust's arguments in support of its relevant positions sound and persuasive. In light of this finding, and given the absence of argument for Microsoft's positions, the Court now adopts InterTrust's proposed constructions for all thirteen of these terms and phrases, other than "budget" and "securely applying . . . said data item."[13]

Aside from the Court's adoption of InterTrust's proposed constructions, the Court wishes to make clear that Microsoft's failure to brief these terms and phrases has serious implications. Microsoft has chosen to dispute these terms and phrases, and it has supplied the Court with proposed constructions. In so doing, Microsoft's attorneys are bound to comply with Rule 11(b), which provides in pertinent part:

> By presenting to the court (whether by signing, filing, submitting, or later advocating) a pleading, written motion, or other paper, an attorney or unrepresented party is certifying that to the best of the person's knowledge, information, and belief, formed after an inquiry reasonable under the circumstances, . . . [¶] the allegations and other factual contentions have evidentiary support or, if specifically so identified, are likely to have evidentiary support after a reasonable opportunity for further investigation or discovery . . . .

Fed. R. Civ. P. 11(b). Thus, by asserting that the terms and phrases at issue should be defined as proposed by Microsoft, Microsoft's attorneys are representing to the Court that these terms and phrases have evidentiary support. Microsoft's failure now to provide any discussion whatever on these terms and phrases in its Markman brief arguably suggests that Microsoft's attorneys never had

---

[12] Microsoft has no excuse for failing to provide briefing on these terms and phrases. That InterTrust was able to present in its Markman brief cogent arguments on all thirty terms and phrases, as well as the global construction of "virtual distribution environment," see infra, demonstrates that the 40 pages that the Court granted Microsoft to brief its positions were sufficient to address all terms and phrases in dispute.

[13] The Court excepts these two terms and phrases because Microsoft did brief terms and phrases closely related to these two terms, namely the phrase "a budget specifying the number of copies which can be made of said digital file" and the term "secure."

sufficient factual basis on which to dispute InterTrust's proposed constructions and to offer their own constructions.

The Court takes this implication very seriously. The Court has expended substantial time and effort on this case. While the Court fully expects that a case of this complexity will require substantial resources and therefore is ready and willing to commit those resources to achieve a proper resolution of this matter, the Court is not willing to waste its time attempting to resolve issues that are not disputed in good faith. Thus, if Microsoft's counsel did not deem Microsoft's positions on the thirteen terms and phrases sufficiently important or well-founded to brief, they should not have presented them to the Court for consideration in the first place. Microsoft and its counsel are hereby admonished not to waste the Court's time in this or any similar way in the future.

Accordingly, the Court CONSTRUES the following terms and phrases as set out below.

a. <u>Aspect</u>

"Aspect" means: "Feature, element, property, or state."

b. <u>Authentication</u>

"Authentication" means: "Identifying (<u>e.g.</u>, a person, device, organization, document, file, etc.). Authentication includes uniquely identifying or identifying as a member of a group."

c. <u>Clearinghouse</u>

"Clearinghouse" means: "A provider of financial and/or administrative services for a number of entities; or an entity responsible for the collection, maintenance, and/or distribution of materials, information, licenses, etc."

d. <u>Compares</u>

"Compares" means: "Examines for the purpose of noting similarities and differences."

e. <u>Derive</u>

"Derive" means: "Obtain, receive, or arrive at through a process of reasoning or deduction. In the context of computer operations, the 'process of reasoning or deduction' constitutes operations carried out by the computer."

f. <u>Designating</u>

"Designating" means: "Indicating, specifying, pointing out, or characterizing."

g. Device Class

"Device class" means: "A group of devices which share at least one attribute."

h. Digital Signature/Digital Signing

"Digital signature" means: "A digital value, verifiable with a key, that can be used to determine the source and/or integrity of a signed item (e.g., a file, program, etc.)." "Digitally signing" is the process of creating a digital signature.

i. Digitally signing a second load module with a second digital signature different from the first digital signature, the second digital signature designating the second load module for use by a second device class having at least one of tamper resistance and security level different from the at least one of tamper resistance and security level of the first device class

"Digitally signing a second load module with a second digital signature different from the first digital signature, the second digital signature designating the second load module for use by a second device class having at least one of tamper resistance and security level different from the at least one of tamper resistance and security level of the first device class" means:

> Generating a digital signature (i.e., a digital value, verifiable with a key, that can be used to determine the source and/or integrity of a signed item (e.g., a file, program, etc.)), for the second load module, the digital signature designating (i.e., indicating, specifying, pointing out, or characterizing) that the second load module is for use by a second device class (i.e., a group of devices which share at least one attribute). The second device class must have a different tamper resistance (defined infra) or security level than the first device class.

j. Executable Programming/Executable

"Executable programming" and "executable" mean: "A computer program that can be run, directly or through interpretation."

k. Identifying at least one aspect of an execution space required for use and/or execution of the load module

"Identifying at least one aspect of an execution space required for use and/or execution of the load module" means: "Identifying an aspect (i.e., a feature, element, property, or state) of an execution space that is needed in order for the load module to execute or otherwise be used."

2. Remaining Terms and Phrases for Construction

Microsoft provided briefing on 17 of the 30 terms and phrases, as well as the issue of

whether the term virtual distribution environment should be read into every claim at issue. Nevertheless, as the Court informed the parties at the mini-Markman hearing, the Court's consideration of most of Microsoft's arguments has been substantially hampered by Microsoft's persistent failure to provide evidentiary and legal citations in support of these arguments. Page after page of Microsoft's Markman Brief contains bold assertions about the meaning of certain claim terms that have few supporting authorities, and the authorities that do appear generally do not provide support for the dispositive arguments that Microsoft is asserting. (E.g., Microsoft's Markman Br. at 37, 39–40.) Without such evidentiary or legal citations, the Court has little basis to credit Microsoft's assertions.

Microsoft cannot reasonably contend that the 40 pages it was allocated for its Markman brief was insufficient for it to provide such citations, as InterTrust was able to present all of its pertinent arguments with adequate supporting citations in the 40 pages it was allocated for its opening Markman brief. Nor can Microsoft reasonably expect the Court to comb through Microsoft's voluminous submissions to locate authority that might support its specific assertions where Microsoft has failed to refer the Court to specific pages and passages in those submissions. Nor could Microsoft reasonably expect to be able to raise new arguments or cite to new authorities for the first time at the mini-Markman hearing, other than to respond to arguments or authorities appearing for the first time in InterTrust's reply brief. As far as the Court is concerned, the persuasiveness of an argument in support of a proposed construction is in direct proportion to the authorities on which it is premised. Necessarily this means that an argument that lacks appropriate supporting citations is no argument at all. Thus, Microsoft cannot be heard to complain that the Court has not adequately considered its arguments where these arguments are insufficiently supported by citations to evidentiary and/or legal authorities.

With the foregoing in mind, the Court turns to its consideration of the 17 terms and phrases briefed by Microsoft, the two terms and phrases not construed above, and the "global construction" of virtual distribution environment asserted by Microsoft.

a. Global Construction of Virtual Distribution Environment (VDE)

At the outset, there is some uncertainty over Microsoft's position about the global

construction of virtual distribution environment ("VDE"). In Exhibit A to the JCCS, Microsoft indicates that its position is that each of the seven claims at issue in this mini-Markman proceeding should be construed to incorporate a VDE. More specifically, Microsoft states with respect to nine of the twelve claims: "Claim as a whole: The recited method is performed within a VDE." (JCCS Ex. A at 1 (¶ 1), 9 (¶ 14), 11 (¶ 25), 13 (¶ 38), 20 (¶ 65), 26 (¶ 74), 28 (¶ 81), 36 (¶ 98), 39 (¶ 110) (underscoring in original) (boldface omitted).) Microsoft offers similar pronouncements with respect to the remaining three claims. (See id. at 15 (¶ 51), 24 (¶ 70), 30 (¶ 86).) Further, Microsoft asserts the following in its Markman brief:

> The claims must be read in light of the entire 900+ page "Big Book" patent application and, in particular, its 115 page "Summary of the Invention." This Summary of the Invention makes literally hundreds of statements touting the "important," "fundamental," "critical," and required features, capabilities and purposes of the "present invention." The Summary further defines this "invention" (which it expressly names "VDE") by distinguishing it from the allegedly "limited" and rigid solutions of others. All of these are required aspects of the "present invention," not merely optional features of a "preferred embodiment." As such, the claims must be read to include these "invention" features.

(Microsoft's Markman Br. at 1 (emphasis added).) Microsoft states elsewhere in its Markman brief that it "asks the Court to construe each claim as requiring the disclosed 'invention,' as it has been distilled in Microsoft's global 'claim as a whole' construction." (Id. at 5 (emphasis added).) It emphasizes additionally: "[T]he claim construction point being made by Microsoft is that all of these claims necessarily invoke the required 'features' of the VDE 'invention,' not that all claims require only those features. InterTrust's patent claims are free to recite additional features, which additional limitations may (or may not) make them separate 'inventions' under Patent Office restriction practice." (Id. at 15 (emphasis added).)

In its Markman briefing InterTrust purports to interpret Microsoft's position, probably as a result of these statements, to be that every claim impliedly includes a limitation of VDE—that is, there should be a global construction of VDE. (See, e.g., InterTrust's Opening Markman Br. at 7.) Microsoft does not indicate in its Markman brief that InterTrust has mischaracterized its position.

Based on Microsoft's statements in its Markman brief and JCCS and the fact that Microsoft did not take exception to InterTrust's characterization of Microsoft's position, the Court reached the same understanding of Microsoft's position that InterTrust purported to reach. At the mini-

Markman hearing, however, counsel for Microsoft claimed for the first time that InterTrust had mischaracterized its position. According to counsel, Microsoft was not contending that VDE should be read into each claim as a limitation; rather, each disputed claim term should be accorded the meaning that it has in the VDE context. (Transcript of Proceedings, Claims Construction Hearing ("Tr.") 59:2–8.)

The Court finds Microsoft's position at the mini-Markman hearing to be fundamentally different from, and not reasonably supported by, its statements in its written submissions. Microsoft repeatedly states in the JCCS that for each claim as a whole, the recited method is performed within a VDE. In addition, Microsoft states in its Markman brief that every claim must contain all features of a VDE. These pronouncements cannot be interpreted to mean anything other than that the scope of each claim is limited by all the features of a VDE. In other words, Microsoft's written statements evince the view that even if every express element of one of the claims at issue reads on an accused device, that device would still not infringe the claim if the device did not have all the features that Microsoft claims to be the hallmark of VDE. If Microsoft wished to advance the position that it presented at the hearing, it could have easily done so in its papers by stating that "each disputed claim term must be construed in accordance with its meaning in the context of VDE." At the very least, it should have alerted the Court in its Markman brief that InterTrust in its opening brief had mischaracterized Microsoft's position. Microsoft will not be heard to complain that the Court misapprehends its position where it has made affirmative representations to the Court about its position and remains silent when InterTrust purports to interpret its position consistent with those representations. The Court thus proceeds to consider the parties' arguments with the understanding that Microsoft's position is that each claim is limited by all the features of a VDE.

Microsoft contends that each claim at issue impliedly contains a limitation of VDE, even though the term VDE appears in only one of the twelve claims, 900.155, and, then, only in its preamble. The proper construction of VDE is addressed infra in Part III.B.2.t. Microsoft's argument rests on the apparent fact, which is not contested by InterTrust, that all seven of the patents-in-suit that are the subject of the mini-Markman proceeding derive from the 900-page "Big

Book" patent application submitted to the Patent Office in or about 1995.[14] Microsoft focuses on the repeated references to the "invention" and VDE in the specifications of these patents, arguing that the claims necessarily contemplate that VDE will be an additional limitation read into all the claims.

InterTrust disagrees with Microsoft's assertions, making a few key arguments. First, InterTrust points out that the eleven claims other than 900.155 contain no limitations relating to VDE. Citing a pair of Federal Circuit cases, Amgen Inc. v. Hoechst Marion Roussel, Inc., 314 F.3d 1313 (Fed. Cir. 2003), and Renishaw PLC v. Marposs Societa' Per Azioni, 158 F.3d 1243 (Fed. Cir. 1998), InterTrust argues that statements in an application regarding the invention cannot be read into the claims absent a relevant limitation in the claims themselves. (InterTrust's Opening Markman Br. at 9.) Second, citing, inter alia, Amgen, InterTrust argues that it is improper to read into claims a limitation from the specification that does not clearly and unambiguously exclude or disclaim certain embodiments. (Id. at 9–10.)

Third, InterTrust contends that specification statements about the "invention" do not limit the claims if the rest of the specification and file history do not indicate that such a limitation was intended; and InterTrust urges that several aspects of the specification and file history contradict an importation of VDE into all the claims. (Id. at 10–11.) Specifically, InterTrust points out that the PTO held that the Big Book application claimed five separate categories of invention, forcing it to restrict its application to one class of inventions to be pursued in the application. (Id. at 11–13.) InterTrust followed the PTO's command, and also filed separate "divisional" applications relating to the other categories of inventions pursuant to 35 U.S.C. § 121.[15] (Id. at 12.) In addition, InterTrust calls the Court's attention to the '876 patent, which is not one of the seven patents-in-suit that are

---

[14] According to Microsoft, the specification of the '193 patent publishes the Big Book specification without any substantive additions, and therefore Microsoft frequently cites to the '193 specification as a proxy for the Big Book. (Microsoft Markman Br. at 16.) InterTrust states that the '193, '891, and '912 have specifications identical to that of the Big Book, and the '900 patent is a continuation-in-part and also includes all of the text from the original application. (InterTrust's Opening Markman Br. at 12.)

[15] 35 U.S.C. § 121 provides in part: "If two or more independent and distinct inventions are claimed in one application, the Director [of the Patent and Trademark Office] may require the application to be restricted to one of the inventions. If the other invention is made the subject of a divisional application which complies with the requirements of section 120 of this title it shall be entitled to the benefit of the filing date of the original application."

the subject of the mini-Markman hearing but is one of the eleven patents-in-suit asserted by InterTrust. InterTrust explains that the '876 patent issued as a direct continuation of the Big Book application and, therefore, includes the same specification as the '193 patent, including the same statements regarding the "invention" and VDE that Microsoft has cited. (Id. at 13–14.) The '876 patent includes numerous dependent claims adding an express requirement that a process or method include a VDE. (Id. at 14.) These claims, Microsoft maintains, demonstrate that the claims do not recite a VDE, since otherwise the inclusion of the term VDE would be redundant.

Having thoroughly considered the parties' arguments in their papers and the arguments of counsel at the hearing, the Court concludes that Microsoft's position must be rejected. The PTO's determination that the Big Book application described five inventions is alone dispositive.[16] The PTO's decision makes clear that these five inventions are separate, independent, and discrete from one another, each capable of existing in the absence of the rest:

> The inventions are distinct, each from the other because of the following reasons:
>
> 2. Inventions of Groups I-V are related as subcombinations disclosed as usable together in a single combination. The subcombinations are distinct from each other if they shown to be separately usable. In the instant case, invention of Group I has separate utility such as protecting executable code from computer viruses. Invention of Group II has separate utility such as a computer network administration. Invention of Group III has separate utility such as protection of software. Invention of Group IV has separate utility such as a contract bidding procedure. Invention of Group V has separate utility such as auditing of pay television.
>
> 3. Because these inventions are distinct for the reasons given above and have acquired a separate status in the art as shown by their different classification, restriction for examination purposes as indicated is proper.
>
> 4. Because these inventions are distinct for the reasons given above and have acquired a separate status in the art because of their recognized divergent subject matter, restriction for examination purposes as indicated is proper.

---

[16] The Court clarifies that, in reaching this conclusion, it needs not and does not rely on the reasoning of Rambus Inc. v. Infineon Technologies AG, 318 F.3d 1081 (Fed. Cir. 2003), a case of superficial apposition cited by InterTrust. In Rambus, the Federal Circuit found that a specific claim term should not have been read into the claims of a patent resulting from a divisional application that was filed after the PTO found that the original application claimed more than one invention. Rambus, however, is readily distinguishable because in that case the PTO specifically identified the claim term at issue and expressly defined a divisional category of inventions that excluded that claim term, see id. at 1086; the analogy here would be if the PTO had separated the five categories of inventions claimed through the Big Book based on whether or not they were limited to a VDE. Such is not the case here, and thus the Court does not rely on Rambus in considering the significance of the PTO's ruling on the Big Book.

United States District Court
For the Northern District of California

(JCCS Ex. C at 103 (24(BB) ('193 file history, Sept. 25, 1996 Office Action at 2–3)).) The foregoing makes unequivocal that the PTO determined that the Big Book described multiple independent inventions, each with separate utility, each with separate subject matter. Given this determination, it is impossible to conclude that, as Microsoft maintains, every claim must be read to contain all the features of a single "invention," namely the "invention" allegedly described in the Big Book application.

At the hearing counsel for Microsoft invoked Netword, LLC v. Centraal Corp., 242 F.3d 1347, 1352 (Fed. Cir. 2001), for the proposition that "claims cannot enlarge what's patented beyond what the inventor described as the invention." (Tr. 62:7–10.) Counsel appropriately cited to Netword for this principle, 242 F.3d at 1347, and the Court does not disagree with its validity. But this general principle is not inconsistent with the conclusion that the Big Book application described five independent and discrete inventions and, accordingly, the Court's instant determination that each of the claims at issue should not be read to include VDE. As Netword makes clear, the focus is on what the inventor described to the PTO as the invention, not what the inventor may have subjectively believed to be the invention. Here, the inventors submitting the Big Book evidently described five separate inventions. Reading this description and reaching this conclusion, the PTO ordered the inventors to restrict their application to one of the five inventions and to pursue divisional applications if they so chose. The inventors submitting the Big Book may very well have subjectively believed that there was but a single invention, but their subjective beliefs and intent are of no moment.

The Court also finds compelling InterTrust's invocation of the '876 patent. As InterTrust notes, the '876 patent issued as a direct continuation of the Big Book application; it includes the same specification as the '193 patent. Accordingly, one would expect that Microsoft's "global construction of VDE" argument would be equally applicable to construction of the '876 patent. Indeed, as Microsoft argues in its Markman brief, "related patents should be construed consistently." (Microsoft's Markman Br. at 16.) Yet several of the claims in the '876 patent, including claims 10 through 14, expressly contain a VDE limitation. If, as Microsoft asserts, VDE should be implicitly read into all claims within all patents directly derived from the Big Book application, these claims'

express VDE limitation appears redundant and nonsensical.[17]

Still further, much of Microsoft's theory for construing all the claims at issue to incorporate Microsoft's conception of VDE rests on conclusory reasoning. For example, Microsoft contends in its Markman brief:

> Contrary to InterTrust's position (InterTrust Br. at 8:9-10), all four '193 Patent mini-Markman claims concern the distribution and protection of digital content, and contemplate multiple nodes and participants. Information is received (possibly from multiple upstream content providers), then stored on a device having unspecified authorized and unauthorized users, and then conditionally transferred to another device having unspecified users. The claims promise to control three forms of unauthorized use of this distributed content: copying, distributing (to the second device), and storing (on the first and/or second device):
>
> > "if said copy control allows at least a portion of said digital file to be copied and stored on a second device...." ('193 321:10-11)
> >
> > "determining" or "determine" "whether said digital file may be copied and stored on a second device ...." ('193 321:7-9)
>
> This claim language (e.g., "if ... allows," "determining whether") is not qualified. It implies that if the copying and storing are not allowed, then they are prevented (see Reiter Depo. at 174:1-178:11), no matter what effort may be made to take the unauthorized action. In other words, these claims imply that their "controls" are effective in the face of the attacks identified in the Big Book.

(Microsoft's Markman Br. at 16–17.) As InterTrust correctly notes in its reply, nothing that Microsoft has cited to the Court indicates that the claims require multiple upstream content providers, multiple users of the first device, or multiple users of the second device. (InterTrust's Reply Markman Br. at 8.) Moreover, nothing in the language from the '193 patent specification

---

[17] At the hearing Microsoft objected to the introduction of the text of the '876 patent in connection with the construction of the claims at issue. Microsoft contended that the '876 patent constitutes extrinsic evidence that should not be considered unless the Court finds the claim terms ambiguous. (Tr. 68:6–22.)

This objection is untimely. Microsoft had fair notice from InterTrust's Markman briefs that InterTrust was relying on the '876 patent, and it had ample opportunity to file objections to evidence prior to the hearing (as InterTrust did), yet Microsoft declined to do so. At any rate, to the extent that consideration of the '876 patent is appropriate only if the Court finds the claim terms ambiguous, this condition has been met: notwithstanding Microsoft's last-minute attempted about-face in its "global construction of VDE" position, the Court has construed that position to be that each claim must be read as containing a limitation of VDE, and this position presents an ambiguity—that each claim must implicitly contain a limitation not explicitly stated. Finally, Microsoft has effectively waived this objection by affirmatively arguing that related patents must be construed consistently. Accordingly, the Court OVERRULES this objection.

cited above implies that "if the copying and storing are not allowed, then they are prevented . . . , no matter what effort may be made to take the unauthorized action." The Court has also read the cited portion of Dr. Reiter's deposition testimony, and if fails to understand how this testimony supports this proposition. Nor does the language quoted from the '193 patent specification imply that the claims' "'controls' are effective in the face of the attacks identified in the Big Book."

Finally, as an intuitive and legal matter, the Court is wary of reading into claims a limitation that is not expressly there. As InterTrust correctly notes, "[s]pecifications teach. Claims claim." SFI Int'l v. Matsushita Elec. Corp. of Am., 775 F.2d 1107, 1121 n.14 (Fed. Cir. 1985). With its global construction argument, Microsoft is not asking for construction of a term; it is asking for wholesale importation of a term that is present in only one of the claims at issue. In the absence of substantial justification for Microsoft's position, the Court is disinclined to take such a drastic step. See Comark Communications, Inc. v. Harris Corp., 156 F.3d 1182, 1186–87 (Fed. Cir. 1998) (holding improper reading into claims a limitation appearing only in the specification).

For all of these reasons, the Court CONSTRUES the claims at issue as not impliedly incorporating the features of a VDE as a limitation.

b. Budget

InterTrust asserts that its proposed construction of the term "budget" (appearing in 193.1), "information specifying a limitation on usage," reflects the plain English meaning of the word. (InterTrust's Opening Markman Br. at 16.) In contrast, Microsoft's proposed construction of budget requires it to be a unique type of "method" that specifies a decrementable numerical limitation on future use, where "use" is defined separately. InterTrust assails Microsoft's proposal by citing examples in the specification where the terms "budget" and "BUDGET method" are used separately and arguing that, in light of these examples, budget cannot imply a method without being nonsensical. (See id.) InterTrust also portrays Microsoft's definition as being based on the preferred embodiment in the patent, and it argues that reading limitations from preferred embodiments in specifications into claims contravenes appropriate claim construction practice. (See id. at 16–17 (citing Laitram Corp. v. Cambridge Wire Cloth Co., 863 F.2d 855, 865 (Fed. Cir. 1988)).) InterTrust further adds that there is no basis in the specification to read into the definition

that budget must be a decrementable numerical limitation. (Id. at 17.)

In its Markman brief, Microsoft does not present any arguments for the term budget, although it discusses the larger phrase "a budget specifying the number of copies which can be made of said digital file." (Microsoft's Markman Br. at 38–39.) Its discussion of this phrase is very brief, however: it asserts only that its construction of this phrase, which incorporates the term budget, answers the questions "can be made since when?" or "by whom?" or "by what?" (Id.)

Given Microsoft's failure to advance any argument specifically directed to its proposed definition of the term budget, the Court has no basis to adopt Microsoft's position. Moreover, the Court finds InterTrust's proposed definition of budget to be reasonable and its criticisms of Microsoft's proposal to be cogent and compelling. Accordingly, the Court adopts InterTrust's proposal and CONSTRUES the term "budget" to mean: "Information specifying a limitation on usage."

c. **A budget specifying the number of copies which can be made of said digital file**

InterTrust's proposed definition of the phrase "a budget specifying the number of copies which can be made of said digital file" (193.1) uses the normal English meanings of the words, but it incorporates the separately defined terms budget and copies. (InterTrust's Opening Markman Br. at 21.) Microsoft's definition of the phrase incorporates the term budget, requires the budget to state "the total number of copies (whether or not decrypted, long-lived or accessible)," and requires that "[n]o process, user, or device is able to make another copy of the Digital File once this number of copies has been made." InterTrust criticizes the requirement that the budget state the total number of copies as unsupported by the claim term and as nonsensical. (Id.) InterTrust also contends that the requirement that no process, user, or device be able to make another copy of the digital file once the specified number of copies have been made, is inconsistent with the specification. (Id.) Microsoft responds only by claiming that its construction answers the questions "can be made since when?" or "by whom?" or "by what?" (Microsoft's Markman Br. at 38–39.)

The Court has no basis to adopt Microsoft's proposal. Microsoft does not explain why it is necessary to read into claims utilizing this phrase a limitation addressing when, by whom, or by

what copies can be made of a digital file. No reason is evident. By contrast, InterTrust's definition is commonsensical. Accordingly, the Court adopts InterTrust's definition and CONSTRUES the phrase "a budget specifying the number of copies (defined infra) which can be made of said digital file" to mean: "a budget (i.e., information specifying a limitation on usage) stating the number of copies that can be made of the digital file referred to earlier in the claim."

d. Component Assembly

The parties agree that "component assembly" (912.8, 912.35) has no ordinary meaning in the art. InterTrust's proposed definition is "two or more components associated together," where components "are code and/or data elements that are independently deliverable"; InterTrust explains that component assemblies "are utilized to perform operating system and/or applications tasks." Microsoft proposes a definition that is extremely lengthy—far too long to be suitable for reproduction here.

InterTrust asserts that its proposed construction "is taken directly from the manner in which the term is used in the specification and file history." (InterTrust's Opening Markman Br. at 38.) It cites to examples in the relevant specifications. (Id. (citing JCCS Ex. C at 18 (6(A) ('193 patent at 83:12–26), 6(B) ('193 patent at 83:43–48)), 21 (6(K) ('912 patent file history, Sept. 22, 1998 Office Action at 2–3))).) InterTrust argues that certain limitations that Microsoft reads into its proposed construction are preferred embodiments, not claim elements, and this practice is improper. (Id.) It further argues that Microsoft's proposed limitation that a component assembly be assembled and executed in a "Secure Processing Environment" is directly contradicted by the specification, which states that this condition is merely an option. (Id. at 38–39.)

Microsoft's sole argument is that the only type of "component assembly" mentioned in the Big Book is the kind identified in Microsoft's proposed construction, and therefore this construction should be adopted. (Microsoft's Markman Br. at 36.) Microsoft, however, provides no citations in support of the assertion that component assembly is "uniformly" used in the Big Book to refer to executable components. (Id.) In its reply, InterTrust allows that it "did not intend to leave open the possibility that a component assembly might include no programming." (InterTrust's Reply Markman Br. at 21.) Accordingly, InterTrust states that it "is willing to amend the third sentence of

its proposed construction to read as follows: 'Component Assemblies must include code, and are utilized to perform operating system and/or applications tasks.'" (Id.)

Regardless of what the Big Book says, the relevant specifications clearly contradict Microsoft's proposed construction. Moreover, Microsoft fails to provide support for all of the features of its proposed definition. InterTrust's definition, as amended above, is well-supported and reasonable, and the Court adopts it. Accordingly, the Court CONSTRUES "component assembly" to mean: "Two or more components (i.e., code and/or data elements that are independently deliverable) associated together. Component assemblies must include code, and are utilized to perform operating system and/or applications tasks."

e. Contain

The key dispute between the parties is whether "contain" (683.2, 912.8, 912.35) implies that something has within it an actual element (Microsoft's proposal), or whether it may contain either an element or a reference to the element (InterTrust's proposal). InterTrust's proposed construction is based on the plain English meaning of contain. (InterTrust's Opening Markman Br. at 27.) InterTrust further argues that its construction is consistent with the relevant specifications, which explicitly state that a container may "contain" items "without those items actually being stored within the container." (Id. at 28 (citing JCCS Ex. C at 22 (7(B) ('193 patent at 58:48–58))).) Microsoft responds in its Markman brief that such items must actually be stored in a container because Dr. Reiter testified that he could not think of any non-empty digital file that does not contain linked and/or embedded items, and thus all digital files would qualify as containers. (Microsoft's Markman Br. at 39.)

InterTrust's argument is persuasive: the language from the specifications is clear—contain includes having references. Accordingly, the Court adopt's InterTrust's proposal and CONSTRUES "contain" to mean: "To have within or hold. In the context of an element contained within a data structure (e.g., a secure container), the contained element may be either directly within the container or the container may hold a reference indicating where the element may be found."

f. Control (n.)

InterTrust's proposed definition of the term "control" (n.) (193.1, 193.11, 193.15, 193.19,

683.2, 891.1) relies primarily on the plain English definition of the word and on the specifications. (See InterTrust's Opening Markman Br. at 17–19.) The specifications, according to InterTrust, equate control with "control information," and it provides examples of these terms that include both data and executable files. (Id. at 17–18.) InterTrust also cites to excerpts from the '193 and related file histories that suggest that a control can be a data file. (Id. at 18.) InterTrust assails Microsoft's proposed definition for requiring a control to be executable (see infra), noting that the specifications demonstrate that a control can be data, which are not executable. (Id.) InterTrust also criticizes Microsoft's proposal for requiring a secure processing environment ("SPE"), contending that the patents make clear that requiring an SPE is but a limitation in a particular embodiment, and the patents disclose an alternate embodiment known as a host processing environment. (Id.) InterTrust adds that Microsoft's requirement that control implies the ability to modify controls is but a preferred embodiment, and in any event it is a capability provided by a particular operating system described in the specification. (Id.) Finally, InterTrust objects to Microsoft's apparent application of the general definition of control to the term "user control," which, InterTrust argues, was on the parties' initial list of claim terms to be construed for the mini-Markman proceeding but was not selected. (Id. at 18–19.)

Microsoft proposes an extraordinarily lengthy definition of control that reflects the alleged use of the term in the Big Book. First, it argues that control can be explained with an analogy to a rare books library holding valuable texts, where each type of access is controlled by a different set of rules, such as a particular type of guard performing a particular function. (Microsoft's Markman Br. at 37.) Once again, Microsoft provides no citations in support of this proffered analogy. (Id.) Second, Microsoft refers to the Big Book, suggesting that the sense in which "control" is used therein should be applied to the claims at issue. (Id. at 37–38.) Third, Microsoft assails InterTrust's argument that "rules and controls" are equated with "control information," pointing out that the patent specifications distinguish between rules and controls, such as by using the phrase "rules and/or controls." (Id. at 38.)

InterTrust's arguments are generally well-supported and convincing. Microsoft's are not. The Court is not disposed to credit Microsoft's "rare books library" analogy where Microsoft has

declined to take the time to provide any citations in support of it, nor will the Court accept counsel's entreaty at the hearing to divine an evidentiary basis from the sparse citations in the 36 pages appearing in Microsoft's brief before this analogy, (see Tr. 78:2–12). As for Microsoft's reliance on the Big Book, Microsoft's quotations of excerpts from the specifications demonstrate only that a control may be executable; they do not demonstrate that a control may not be non-executable. (See Microsoft's Markman Br. at 37–38.) Given that InterTrust's proposed construction allows for both executable and non-executable programming, this evidence is fully consistent with InterTrust's proposed definition.

Microsoft's only point that merits attention—a point criticizing InterTrust's proposal, not supporting Microsoft's—is its attempt to distinguish between rules and controls, and thereby its attempt to distinguish control and control information, by invoking the specifications' references to "rules and/or controls." These references to rules and controls both in the conjunctive and disjunctive may well seem to suggest that rules are distinct from controls, and thus controls cannot be equivalent to control information if, as InterTrust urges, control information is also equivalent to rules. Nevertheless, the evidentiary support cited by InterTrust is sufficient to overcome the Court's concerns. In particular, the specification for the '193 patent clearly uses control and control information interchangeably, (see JCCS Ex. C at 24 (8(C)) ('193 patent at 129:52–60)), and the file histories of the '193 patent and the '683 patent demonstrate that control is used to mean data, (id. Ex. C at 31–32 (8(W)), 32 (8(X)), 33 (8(AA))). InterTrust has thus established that control is equivalent to control information. That is the key to the Court's resolution of this issue: once this identity is established, the remaining evidence cited by InterTrust provides ample support for its position. The Court need not resolve whether "rule" has a meaning independent from control. Even if the Court were to attempt to do so, Microsoft does not provide any evidence as to what that independent meaning might be; its assertion that "[i]n the Big Book's usage, a 'rule' need not be executable, but a 'control' must be," is bereft of supporting citations. Without such evidence, the Court cannot ascribe to the phrase "rules and/or controls" a significance that would call into question the aptness of InterTrust's proposal.

Accordingly, the Court adopt's InterTrust's proposed definition and CONSTRUES "control"

(n.) to mean: "Information and/or programming controlling operations on or use of resources (e.g., content) including (a) permitted, required, or prevented operations, (b) the nature or extent of such operations, or (c) the consequences of such operations."

g. **Controlling, Control (v.)**

InterTrust asserts that "control" (v.) (193.1, 861.58) does not have any special meaning in the specifications. (InterTrust's Opening Markman Br. at 21.) Its proposed construction is based on the plain English meaning of the word: "to exercise authoritative or dominating influence over; direct." InterTrust criticizes Microsoft's proposed construction as being unduly lengthy and complex, for having no basis in the specification, and for having a particular limitation (the requirement of a VDE SPE) that is actually contradicted by the specifications. (Id. at 22.) Microsoft faults InterTrust's proposed construction as being vague and for promising only "influence" that is inconsistent with the high degree of protection that "the Blue Book promises the owners of content entrusted to VDE." (Microsoft's Markman Br. at 39.) Microsoft also advances an argument about "arbitrary granularity" that is difficult to comprehend. (Id.)[18]

InterTrust's proposed construction is consistent with the specifications. Microsoft's proposed construction does not appear to have any support in the specifications and actually contradicts them. Microsoft's reliance on the supposed promises regarding VDE contained in the Big Book is undercut by the PTO's determination that the Big Book described multiple inventions. Accordingly, the Court adopts InterTrust's sound proposal and CONSTRUES "control" (v.) to mean: "To exercise authoritative or dominating influence over; direct."

h. **Controlling the copies made of said digital file**

The phrase "controlling the copies made of said digital file" (193.1) appears as part of a slightly longer clause in 193.1: "and said at least one copy control controlling the copies made of

---

[18] Specifically, Microsoft states that "'controlling' in this 'invention' is done at an arbitrary granularity, which is an important feature that the Big Book relied upon to distinguish prior art: [¶] 'VDE also extends usage control information to an arbitrary granular level (as opposed to a file based level provided by traditional operating systems)' [citation]." (Id. (citing '193 patent 275:8–11) (emphasis omitted).) Whatever the significance of this statement may be, the cited sentence from the '193 specification is inapposite because it concerns "control information," which is equivalent to the noun form of control. See supra. Here, the Court is construing the verb form of control.

said digital file[.]" InterTrust contends that this phrase is further explained by language appearing later in 193.1, namely: "if said copy control allows at least a portion of said digital file to be copied and stored on a second device." (InterTrust's Opening Markman Br. at 22.) InterTrust maintains that this further description, along with the separately defined incorporated terms, makes clear that the copy control that is controlling the copies made of said digital file, is used to determine whether a digital file may be copied to a second device. (Id.) InterTrust asserts that its definition is based on this straightforward, plain-English interpretation. (Id.)

InterTrust criticizes Microsoft's requirement of a VDE in its construction as not required by the claim and inconsistent with the specification. (Id. at 22–23.) InterTrust also assails Microsoft's definition's requirement that the copy control control "all copies of the Digital File" as not required by the claim. (Id. at 23.) Finally, InterTrust disputes Microsoft's definition's requirement that all uses and accesses be prohibited except to the extent allowed by the copy control(s). (Id.) InterTrust argues that this limitation has no support in the claim and is inconsistent with the specification, which suggests that the item may also be governed by an alternate control structure. (Id. (citing, inter alia, JCCS Ex. C at 116 (26(A) ('193 patent at 28:19–37)), 116–17 (26(B) ('193 patent at 31:29–56))).)

In its response, Microsoft does not affirmatively argue why its definition should be adopted. Rather, it faults InterTrust's definition as reading the claim more as "controlling the copying," even though the claim refers to "controlling the copies." (Microsoft's Markman Br. at 39–40.) Microsoft does not explain the significance of this distinction. (Id.) Microsoft also contends that "InterTrust's proposal suggests that the copies are transferred to the second device, but the claims recite that the file (as opposed to any copy) is transferred." (Id. at 40.) Microsoft does not cite to any authorities in support of these assertions. (Id. at 39–40.)

In its reply brief InterTrust clarifies:

> The InterTrust construction is based on the manner in which this phrase is used in the claim, in which it explains the "copy control." See JCCS Ex. A, Row 7. The nature of the copy control is further described later in the claim. JCCS Ex. A, Rows 8 and 9. InterTrust's definition is based on the phrase itself and on its context in the claim, a context Microsoft entirely ignores.

(InterTrust's Reply Markman Br. at 23.)

InterTrust's proposed construction is sensible and supported by the language of 193.1 and the '193 patent specification. Microsoft has provided no argument in support of why its proposed construction should be adopted. Accordingly, the Court adopts InterTrust's proposed construction and CONSTRUES the phrase "controlling the copies made of said digital file" for purposes of 193.1 to mean: "Determining the conditions under which a digital file may be copied (defined infra) and the copied file stored on a second device."

i. **Copy, Copied, Copying**

InterTrust's proposed construction of the term "copy"[19] and its other permutations (193.1, 193.11, 193.15, 193.19) is based on the plain English meaning of the word. (InterTrust's Opening Markman Br. at 19.) InterTrust's construction, however, requires that the copy be usable, whereas Microsoft's definition allows a copy to be ephemeral, unusable, or inaccessible. (Id.) InterTrust's proposal also allows a reproduction to involve some changes and still be a copy, as long as the essential nature of the content remains unchanged.

InterTrust maintains that the whole point of making a copy is to have it be usable; temporary, automatically-generated internal reproductions of a file by a computer do not fit this description. (See id. at 19–20.) InterTrust adds that construing copies to include such reproductions, which are copies under Microsoft's proposal, would lead to absurd results: a user attempting to utilize a budget (defined supra) by making copies could deplete the entire budget on these ephemeral reproductions without being able to use any of them. (Id. at 20.)

In advancing its proposed definition, Microsoft relies on language from the Big Book, which appears to indicate that a copy need not be usable by everyone. (Microsoft's Markman Br. at 22–23.) Microsoft contends that InterTrust's proposed construction is nonsensical because whether a file is usable and, therefore, whether it is a copy, may change depending on whether a particular user has the ability to use the file. (Id. at 23.) Finally, Microsoft argues that InterTrust's definition contravenes the VDE "invention," which, according to Microsoft, promises prevention of

---

[19] The parties do not distinguish between the noun form and the verb form of this word for purposes of this mini-Markman proceeding.

unauthorized copying, which may take place even if the unauthorized copier could not use the copy. (Id. at 23–24.)

The Court agrees with InterTrust that adopting Microsoft's definition of copy would lead to absurd results because a user might exhaust his entire budget by opening a file without obtaining a single usable copy—and without realizing that he was making a copy every time he opened the file. The Court cannot discern what utility might be gained from this result. At the same time, Microsoft makes a good point that once a "copy" is made, it should not cease being a copy just because it is transferred to someone else who is no longer able to use it. The Court believes that this concern is adequately addressed by adding to InterTrust's definition the requirement that the copy be usable in any way by the person, entity, or device making the copy. Thus, if a copy is made such that it is usable by the person or entity making the copy, and then it is transferred to someone else who is unable to use it, it is still a copy.

It is crucial to understand, however, that "usable" is defined broadly in this definition to mean "capable of any conceivable use," where the noun "use" has its common-English meaning. For example, if a person makes a copy of a digital file that his own computer cannot run for the purpose of e-mailing that file to a friend whose computer can run the file, the copy is still a copy: the person making the copy "used" the file by distributing it to a friend. In other words, a copy is "usable" essentially if it is accessible for any purpose. This understanding of "usable" stands in contrast to Microsoft's apparent understanding of the word. Microsoft seems to take for granted that "usable" (as used in the definition of copy) connotes a certain degree or quality of utility. For example, Microsoft's counsel at the hearing seemed to suggest that a photocopy of a Latin text made by counsel would not be usable by him because he would not be able to read it. (Tr. 221:12–222:3.) By making this assertion, counsel implicitly presumed that the copy would not be usable because it was not comprehensible by the person making the copy. But that premise is not implicit in the word "usable" as it is used in this definition. The copy, whether or not it was comprehensible by the person making the copy, would still be usable if the person making the copy had access to it and could do something with it—perhaps send it to a friend, whether or not the friend's computer could access it. Of course, if the "copy" described by counsel in his analogy fell behind the photocopy

machine before the person making the copy could retrieve it and was no longer accessible, it would not be a "copy" in the sense contemplated by the claims at issue. This requirement is necessary to avoid achieving absurd results. It also illustrates the limitations of the analogy presented by Microsoft's counsel at the hearing.

Finally, the Court agrees with InterTrust that a copy need not be an exact reproduction as long as the essential nature of the content remains unchanged. Surely a user can be said to copy a music file for a song even though he only copies half the song, as long as the resulting copy retains the essential nature of the original song. And, as InterTrust's counsel explained at the hearing, (see Tr. 208:23–209:22), the same user can also be said to copy the music file even if the reproduction he generates is encrypted and thus not an exact duplicate of the original, because the reproduction retains the essential nature of the content of the original.

Accordingly, the Court adopts InterTrust's proposed definition with the aforementioned alteration, such that "copy" (v.), "copied," and "copying" are CONSTRUED to mean, respectively: "Reproduce, reproduced, reproducing, where the reproduction must be usable in any way by the person, entity, or device making the reproduction, may incorporate all of the original item or only some of it, and may involve some changes to the item as long as the essential nature of the content remains unchanged." A "copy" (n.) is such a reproduction.

j. **Derives information from one or more aspects of said host processing environment**

InterTrust's definition of the phrase "derives information from one or more aspects of said host processing environment" (900.155) purports to rely on normal English, incorporating the separately defined terms derive, aspect, and host processing environment. (Id. at 37.) InterTrust argues that the requirement in Microsoft's proposed definition that information be derived from the host processing environment "hardware" is inconsistent with the disclosed embodiment, (id. (citing JCCS Ex. C at 129–30 (29(A) ('900 patent at 239:4–42)))), and finds no support in relevant claim, 900.155, (id.). In response, Microsoft contends, without citation or clear explanation, that InterTrust's proposed construction may serve no security purpose at all because it does not require a "unique machine signature" technique allegedly identified by Dr. Reiter. (Microsoft's Markman Br.

at 40.)

InterTrust's proposed definition is sensible and supported by the '900 patent specification. Microsoft has neither provided any support for adopting its proposed definition, nor has it addressed InterTrust's arguments that certain features of its definition are inconsistent with or unsupported by the specification. Accordingly, the Court adopts InterTrust's proposal and CONSTRUES "derives information from one or more aspects of said host processing environment" to mean: "Derives (i.e., obtains, receives, or arrives at through a process of reasoning or deduction) information based on at least one aspect (i.e., feature, element, property, or state) of the previously referred to host processing environment (defined infra)."

k. **Host Processing Environment (HPE)**

In its opening brief, InterTrust maintains that host processing environment ("HPE") (900.155) is explicitly defined in 900.155: it consists of the elements listed in that claim. (JCCS Ex. A at 33 (¶ 87).) InterTrust maintains that HPE therefore needs no additional definition, yet it offers a definition in the alternative. (Id.) Turning to that definition, InterTrust explains it agrees with Microsoft that HPEs may be either secure or non-secure and that InterTrust's proposed definition is more accurately a definition of a secure HPE. (InterTrust's Opening Markman Br. at 36.) It therefore states that if necessary, its proposed construction should be qualified to allow for secure and non-secure HPEs, and it offers language containing such a qualification which it claims to be supported by the specification. (Id.) InterTrust, however, takes issue with Microsoft's inclusion of additional limitations in its proposed definition, arguing that they are unwarranted. For example, InterTrust points out that Microsoft's implicit assertion that an HPE consists only of executable programming contradicts 900.155, which identifies various hardware elements as part of the HPE. (Id.) Microsoft argues in response, without citations to evidence, only that the Big Book permits HPEs to be secure or non-secure, and Microsoft's proposed construction addresses this feature. (Microsoft's Markman Br. at 40.) Microsoft's proposal provides, among other things, that a secure HPE run in "protected (privileged) mode" and that a non-secure HPE run in "user mode."

At the hearing the Court explored InterTrust's offer to qualify its original proposed definition. InterTrust's counsel proposed that the proffered definition be modified to the following:

"[A] host processing environment may be either secure or non-secure. A secure host processing environment is a protected processing environment incorporating software-based security, and a non-secure host processing environment is a processing environment with insufficient security to constitute a secure host processing environment." (Tr. 264:19–24.) Counsel, however, adhered to the position that the Court need not define this term because it consists of the elements of 900.155. (Tr. 265:22–266:14.) Counsel contended that the reference to HPE in 900.155 is similar to a preamble, requiring no construction by the Court, but he admitted that he could not cite to the Court any authority in support of this position. (Id.) Microsoft's counsel responded to InterTrust's amended proposal by arguing that it was nonsensical to construe HPE to include both secure and non-secure processing environments because an HPE is a type of protected processing environment. (Tr. 268:21–269:12.) He cited portions of the '193 patent specification in support of this position. (Tr. 269:18–271:10.) Microsoft's counsel admitted, however, that Microsoft's own proposed definition allowed for HPE to be both secure and non-secure. (Tr. 273:21–274:1.) InterTrust's counsel commented that the key difference between InterTrust's revised proposal and that of Microsoft was that Microsoft's proposal requires that an HPE run in protected mode. (Tr. 272:12–14.) He went on to assert that there is no statement in the '193 patent that suggests that a secure HPE or a non-secure HPE must operate in a particular mode. (Tr. 272:15–273:7.)

The Court fully understands InterTrust's position that the reference in 900.155 to HPE is akin to a preamble requiring no construction, as that reference appears on the second line of the claim without any other elements. Yet given the references to HPE in conjunction with protected processing environments and secure processing environments in the specifications of the '193 patent and the '900 patent, (JCCS Ex. C at 56 (16(B) ('193 patent at 105:18–22, '900 patent at 112:48–52))), the Court considers it to have significance independent from the remaining elements of 900.155 themselves. The Court thus construes HPE accordingly.

Microsoft's proposed definition is not plausible. Microsoft provides no support for the requirement that HPE be "within a VDE node" or for the requirement that a secure HPE run in protected mode and a non-secure HPE run in a different mode. InterTrust's revised proposal, on the other hand, properly incorporates the term "protected processing environment" (defined infra)

consistent with HPE's use in the specifications. Moreover, the Court does not agree with Microsoft's suggestion that InterTrust's proposed definition is nonsensical because there cannot be a non-secure protected processing environment. A protected processing environment is a separately defined term that, under InterTrust's proposed definition, provides protection against tampering. (See JCCS Ex. B at 11 (¶ 18).) InterTrust's proposed definition of tampering (a term that is not offered for construction by the Court but will be implicitly defined in the Court's construction of "tamper resistance") is not coextensive with its proposed definition of secure. (Compare id. Ex. B at 15 (¶ 21) with id. Ex. B at 13 (¶ 19).) Given that, as discussed infra, the Court adopts InterTrust's proposed definitions of secure and tamper resistance, there is no inconsistency in concluding that HPEs may be secure and non-secure. Moreover, Microsoft's own proposed construction of HPE allows it to be either secure or non-secure.

Accordingly, the Court adopts InterTrust's revised proposal and CONSTRUES "host processing environment" (and its acronym, "HPE") as follows: "A host processing environment may be either secure or non-secure. A secure host processing environment is a protected processing environment (defined infra) incorporating software-based security, and a non-secure host processing environment is a processing environment with insufficient security to constitute a secure host processing environment.

l. **Identifier**

InterTrust contends that its proposed construction of "identifier" (193.15, 912.8) is based on the normal English meaning of the term and is consistent with its use in the specifications. (InterTrust's Opening Markman Br. at 24.) InterTrust asserts that the main dispute between the parties is whether, as Microsoft contends, identifier must be unique to an "individual instance" of a person or thing, or whether, as InterTrust contends, it can specify that a person or thing is a member of a group. (Id.) InterTrust points to a specification embodiment of a portion of 912.8 that appears to lend support to its construction. (Id. (citing JCCS Ex. C at 131 (30(A) ('193 patent at 140:15–46))).) Microsoft in response does not address identifier, but rather "identifying (identify)." (Microsoft's Markman Br. at 40.) Without offering any evidentiary citations in support, Microsoft asserts that "[i]n common usage and these patents, to identify someone or something is to establish

the person or thing as a particular individual or thing." (Id.) In its reply brief, InterTrust objects to Microsoft's construction of the terms "identifying (identify)", contending that they are distinct from identifier and were not agreed-upon as terms that would be construed at the mini-Markman. (InterTrust's Reply Markman Br. at 23 n.13.) InterTrust adds that its proposed construction is based on the American Heritage Dictionary. (Id. at 23.)

InterTrust's arguments are persuasive. Microsoft's argument is unsupported. Accordingly, the Court adopts InterTrust's proposal and CONSTRUES "identifier" to mean: "Information used to identify something or someone (e.g., a password). In this definition, 'identify' means to establish the identity of or to ascertain the origin, nature, or definitive characteristics of; includes identifying as an individual or as a member of a group."

m. Protected Processing Environment (PPE)

InterTrust contends that its proposed construction of "protected processing environment" ("PPE") (683.2, 721.34) is consistent with the specifications, which describe two embodiments of a PPE: a secure processing environment ("SPE") and a host processing environment ("HPE"). (InterTrust's Opening Markman Br. at 28–29.) InterTrust explains that its construction properly covers both embodiments because the specification explicitly states that any action that can be taken by an SPE can also be taken by an HPE, albeit possibly with a lower level of security. (Id. at 29.) InterTrust further contends that a number of Microsoft's proposed definitions would improperly exclude the HPE embodiment, which provides software-based security. (Id.) InterTrust adds that Microsoft's proposed definition of PPE is 345 words in length and thus impossible for any jury to understand. (Id.)

In its Markman brief Microsoft address only what it deems to be the "central dispute": whether a PPE must have a physical tamper resistant barrier (see infra) and prevent unauthorized access, observation, and interference. (Microsoft's Markman Br. at 34.) Although Microsoft's discussion of issues relating to the proper construction of PPE runs a page and a half in length, careful review of this discussion reveals only one substantive argument in support of its proposed definition: that the three reasons provided elsewhere in the brief for adopting Microsoft's construction of tamper resistant barrier also demonstrate that these claims' PPE must be the

hardware-based SPE, not the software-based HPE. (Id. at 35.) Microsoft also faults InterTrust's proposed definition as being "vague" and lacking in more specific information. (Id.)

InterTrust's arguments are persuasive and well-supported. Given that, as discussed infra, Microsoft's tamper resistant barrier arguments are unavailing, so, too, are its arguments regarding PPE. Further, InterTrust's proposed definition is not vague, and Microsoft does not demonstrate that the information that is not provided in InterTrust's definition is crucial. Accordingly, the Court adopts InterTrust's proposal and CONSTRUES "protected processing environment" to mean: "An environment in which processing and/or data is at least in part protected from tampering. The level of protection can vary, depending on the threat. In this definition, 'environment' means capabilities available to a program running on a computer or other device or to the user of a computer or other device. Depending on the context, the environment may be in a single device (e.g., a personal computer) or may be spread among multiple devices (e.g., a network)."

n. Secure, Securely

InterTrust's proposed construction of "secure" and "securely" (193.1, 193.11, 193.15, 683.2, 721.34, 861.58, 891.1, 912.8, 912.35) is flexible and denotes any of several different attributes, including secrecy and authenticity, some or all of which may be applicable depending on the particular context discussed in the specifications. (See InterTrust's Opening Markman Br. at 14–16.) InterTrust assails Microsoft's proposed definition, which requires all of five qualities identified by Prof. Mitchell, as being flatly contradicted by the specifications, which in some contexts make clear that secure connotes fewer than all five of these qualities. (See, e.g., id. at 14 (quoting '193 patent at 233:25–30 ("In one embodiment, the portable appliance 2600 could support secure (in this instance encrypted and/or authenticated) two-way communications with a retail terminal which may contain a VDE electronic appliance 600 or communicate with a retailer's or third party provider's VDE electronic appliance 600.")); see also id. at 14–15.) InterTrust asserts that, as Dr. Reiter has testified, nothing is absolutely secure; InterTrust maintains that its proposed construction reflects this reality, whereas Microsoft's does not. (See id. at 15.)

Microsoft's proposed definition requires that something must have all five of the following qualities to be secure: "availability"; "secrecy"; "integrity"; "authenticity"; and "nonrepudiation."

United States District Court
For the Northern District of California

United States District Court
For the Northern District of California

(Microsoft's Markman Br. at 28.) Microsoft contends that its definition "honors the basic premise of VDE." (Id. at 27.) Microsoft provides no citations whatever in support of its proposal, other than certain extrinsic evidence tending to suggest that secure connotes an absolute state. (Id. at 25–28.) Microsoft criticizes InterTrust's proposal on several grounds (without citations), one of which is that InterTrust's definition, which contains the phrase "one or more mechanisms are employed to . . .", suggests that something can be secure simply if an effort is made, regardless of the result; Microsoft maintains that the term secure connotes a state, regardless of the effort made to achieve that state. (Id. at 26.)

The Court finds InterTrust's proposed definition, for the most part, to be very well supported by the relevant specifications. Microsoft's definition, by contrast, has no evidentiary support and is, in fact, clearly contradicted by the specifications of the patents-in-suit.

But there are a few modifications to InterTrust's proposal that the Court explored with the parties at the hearing and that the Court now deems appropriate to make. First, Microsoft makes a good point that secure connotes a state—albeit not necessarily an absolute state—and not merely an effort. Thus, InterTrust's use of the phrase "one or more mechanisms are employed to . . ." in its proposed construction is potentially problematic. To address this concern, the Court proposed at the hearing modifying this phrase to "one or more mechanisms are employed that . . . ." This alteration indicates that a state has been achieved, not merely that an effort has been made. InterTrust's counsel stated at the hearing that InterTrust had no objection to this modification. (Tr. 121:18–122:1, 149:24–150:1.) Nevertheless, the Court recognizes that a particular mechanism may not by itself prevent, discourage, or detect misuse; rather, it may do so only in conjunction with other mechanisms. Accordingly, the Court believes that a further modification would be helpful: the phrase should read "one or more mechanisms are employed that (whether alone or in conjunction with one or more other mechanisms) . . . ."

Second, the Court agrees with Microsoft's proposal at the hearing—a proposal that counsel later withdrew—that the portion of the last sentence of InterTrust's proposal, namely "but is designed to be sufficient for a particular purpose", should be stricken, such that the sentence shall read: "Security is not absolute." (Tr. 148:14–149:21, 152:20–153:3.) This proposal arose out of the

debate between counsel for InterTrust and counsel for Microsoft about whether something can be secure if it does not guarantee protection against specified threats. Although the Court fully appreciates the distinction that the parties have sought to draw, the Court agrees with InterTrust that security is not absolute and that the language in question adds nothing to the definition and might confuse to a jury. The statement that "security is not absolute" fully captures the meaning sought to be conveyed. Moreover, Microsoft's counsel agreed at the hearing that security is not absolute, (Tr. 141:22 ("So we agree secure is not absolute . . . ."), 152:24 ("[S]aying 'secure is not absolute' . . . [is] a truism . . . ."), and InterTrust's counsel represented that InterTrust was amenable to this modification, (Tr. 149:8–24).

Finally, the Court agrees with Microsoft's concern that defining secure to include mechanisms that merely detect misuse of or interference with information or processes is inappropriate. At the same time, it is clear that the relevant claims contemplate employing security technologies including digital signatures. (See JCCS Ex. C at 74 (19(A)) (citing '193 patent at 8:1–3).) As explained to the Court at the hearing, digital signatures do not provide security by preventing or discouraging misuse of data; instead, they provide security by alerting the user to misuse or interference with the data in question, thereby allowing the user to avoid harm stemming from the misuse or interference. It would thus be inappropriate to exclude detection from the definition of security altogether. The Court believes that it can accommodate Microsoft's concerns while remaining faithful to the meaning of secure contemplated by the patent specifications by modifying "detect" in InterTrust's proposal to "detect misuse of or interference with information or processes for the purpose of discouraging and/or avoiding harm."

Accordingly, the Court adopts InterTrust's proposed definition with the modifications stated above and CONSTRUES "secure" to mean:

///

///

///

///

///

One or more mechanisms are employed that (whether alone or in conjunction with one or more other mechanisms) prevent or discourage misuse of or interference with information or processes, or that detect misuse of or interference with information or processes for the purpose of discouraging and/or avoiding harm. Such mechanisms may include concealment, tamper resistance (defined infra), authentication (i.e., identifying (e.g., a person, device, organization, document, file, etc.)), and access control. Concealment means that it is difficult to read information (e.g., programs may be encrypted). Tamper resistance and authentication are defined separately. Access control means that access to information or processes is limited on the basis of authorization. Security is not absolute.

"Securely" means: "In a secure (defined supra) manner."

o. **Secure Container**

InterTrust's proposed construction of "secure container" (683.2, 861.58, 912.35) is straightforward: a container (defined supra) that is secure (defined supra). InterTrust provides several examples from the specifications that support its proposed construction. (InterTrust's Opening Markman Br. at 26 (citing, inter alia, JCCS Ex. C at 83 (20(A) ('193 patent at 127:30–49)), 84 (20(C) ('683 patent at 15:61–16:4))).) InterTrust also takes issue with a number of features of Microsoft's proposed definition, arguing, inter alia, that it conflicts with the specifications, (id. at 26), that it impermissibly relies on the preferred embodiment, (id. at 27), and that one of its limitations finds no support in the specifications or elsewhere, (id.).

Microsoft proposes a construction of secure container that is enormous in length. Microsoft relies almost exclusively on the alleged Big Book's description of a VDE secure container. (See Microsoft's Markman Br. at 29.) The crucial feature of this proposed type of container is that it prevents, and not simply detects, all access to and use of protected content—i.e., it promises absolute protection. (Id. at 30 ("This 'access control' ability of VDE secure containers is critical to VDE's promise to content owners that it can prevent (not simply detect) all access to and use (not just decryption-based uses) of protected content.").)

InterTrust responds that one feature contained in Microsoft's definition, namely that a secure container includes an access control method, is but an example of an embodiment in the specifications, not the only embodiment disclosed. (InterTrust's Reply Markman Br. at 18.) InterTrust adds that the term "VDE secure container" does not appear anywhere in the '193 patent; when the inventors of that patent wanted to refer to a container in terms of VDE capabilities, they

United States District Court
For the Northern District of California

used the term "VDE container." (Id. at 19.) InterTrust presents examples of the use of the term VDE container. (Id. at 19.)

InterTrust's proposed construction is well-supported by the specifications. Microsoft's proposed construction, which relies on the concept of a VDE secure container, is contradicted by the specifications, as InterTrust demonstrates. In addition, as InterTrust's counsel pointed out at the mini-Markman hearing, Microsoft's counsel's reference to the '193 patent specification in support of its assertion that a VDE container is equivalent to a secure container is misleading: the portion of the specification cited by Microsoft refers only to the preferred embodiment. (Tr. at 238:10–239:11, 240:22 (discussing '193 patent at 127:40–50).)[20] As discussed supra, it is inappropriate for the Court to read limitations in the preferred embodiment into the claim terms. Accordingly, the Court adopts InterTrust's proposal and CONSTRUES "secure container" to mean: "A container (defined supra) that is secure (defined supra)."

p. **Securely applying, at said first appliance through use of said at least one resource said first entity's control and said second entity's control to govern use of said data item**

The phrase "securely applying, at said first appliance through use of said at least one resource said first entity's control and said second entity's control to govern use of said data item" appears only in 891.1. InterTrust contends that "securely applying" is not specially defined in the specification and is not a term of art. (InterTrust's Opening Markman Br. at 34.) InterTrust explains that in the specification, the terms "securely applying" and "applying" refer to the application of control information to govern content. (Id. (citing, inter alia, JCCS Ex. C at 126 (28(A) ('193 patent at 299:19–51))).) InterTrust faults several features of Microsoft's proposed definition for being inconsistent with the specification and/or for lacking support in the specification. (See id. at 34–35.) Microsoft proposes a lengthy definition for this phrase, but it has elected not to address this phrase in its Markman brief.

InterTrust's proposed definition, at least to the extent it relies on a construction of "securely applying" or "applying," has support in the specification. Microsoft has presented no reason to

---

[20] The Court needs not even consider this portion of the '193 specification because Microsoft never cited to it in its Markman brief.

adopt its proposed definition. Accordingly, the Court adopts InterTrust's proposed definition and CONSTRUES "securely applying, at said first appliance through use of said at least one resource said first entity's control and said second entity's control to govern use of said data item" to mean: "The first entity's control (defined supra) and the second entity's control are securely (defined supra) applied to govern use (defined infra) of the data item, the act of securely applying involving use of the resource."

q. Tamper Resistance

InterTrust advances a construction of "tamper resistance" (721.1) that, it contends, is consistent with the use of the term in the specifications and in relevant extrinsic evidence. (InterTrust's Opening Markman Br. at 31.) InterTrust faults Microsoft's proposed definition as requiring that access, observation, and interference be prevented; InterTrust contends that this requirement is inconsistent with the plain meaning of "resistance." (Id.) InterTrust also faults Microsoft's definition as inexplicably requiring prevention of access, which is not connoted by the term "tampering." (Id.)

Microsoft presents little in the way of argument in support of its proposed definition. Microsoft faults InterTrust's definition as failing to specify with what is being compared in connection with the phrase "making tampering more difficult." (Microsoft's Markman Br. at 40.) It also states that "merely detecting tampering but not stopping it, plainly is not what VDE means by 'tamper resistance.'" (Id.) It does not provide any evidentiary or legal citations in support of these statements. (Id.) InterTrust replies in succinct fashion: it states that tamper resistance makes tampering "more difficult" to achieve than it is to achieve in the absence of tamper resistance; and it points out that Microsoft's unsupported assertion about what VDE means by tamper resistance is not evidence supporting Microsoft's construction. (InterTrust's Reply Markman Br. at 24.)

InterTrust's citations to intrinsic evidence, namely the patent specifications, are sufficient to demonstrate that its proposed construction is correct. (See JCCS Ex. C at 87 (21(A) ('721 patent at 4:40–42); 21(B) ('193 patent at 59:48–59)).) Reference to the extrinsic evidence that InterTrust offers is not necessary, although the Court notes that that evidence clearly supports InterTrust's proposed construction. (See, e.g., id. Ex. C at 88 (21(D) (quotation from text on tamper resistant

software that defines such software as "software which is resistant to observation and modification")).) By contrast, Microsoft provides no citations whatever in support of its proposal. There is therefore no basis on which the Court can adopt Microsoft's definition. Accordingly, the Court adopts InterTrust's proposed definition and CONSTRUES "tamper resistance" to mean: "Making tampering more difficult and/or allowing detection of tampering. For purposes of this definition, 'tampering' means using (e.g., observing or altering) in any unauthorized manner, or interfering with authorized use."

r. **Tamper Resistant Barrier**

InterTrust's proposed definition of "tamper resistant barrier" (721.34) is straightforward: "hardware and/or software that provides tamper resistance." InterTrust contends that its definition is consistent with the use of the term in the specification. (InterTrust's Opening Markman Br. at 32–33 (citing JCCS Ex. C at 90 (22(C) ('721 patent at 5:1–6))).) InterTrust further contends that, in accordance with the specifications, its definition permits a tamper resistant barrier to consist of hardware or software. (Id. at 33 (citing JCCS Ex. C at 89–90 (22(B) ('193 patent at 80:22–65))).)

Microsoft claims that its definition, which requires a hardware device and which requires prevention of unauthorized access, observation, and interference, is based on the underlying premise of VDE in the Big Book. (Microsoft's Markman Br. at 30–33.) Microsoft also faults InterTrust's definition of tamper resistant barrier, which incorporates the defined term tamper resistance, as failing to answer the questions "'making tampering more difficult' than what?" and "[w]hat does 'allowing detection of tampering' mean?" (Id. at 34.)

InterTrust points out in its reply that Microsoft's definition's requirement that a tamper resistant barrier include a physical hardware device is contradicted by an express embodiment disclosed in the specification. (InterTrust's Reply Markman Br. at 5–6.) InterTrust states that it "is aware of no Federal Circuit case that has ever held that a claim term can be interpreted to exclude, not merely a disclosed embodiment, but a disclosed embodiment that is identified in the specification using exactly the same words as the claim ('tamper resistant barrier')." (Id. at 6 (emphasis in original).) InterTrust adds that the term is found only in 721.34, and this term contains no reference to assigning usage control information or any use of content, nor does it have any

United States District Court
For the Northern District of California

language from which such elements can be inferred, yet Microsoft's definition includes such elements. (Id. at 19.)

The Court agrees with InterTrust that Microsoft's proposed definition cannot be correct, since it contradicts the use of the term in an embodiment expressly disclosed in the relevant specifications. Indeed, language from one of the specifications that Microsoft itself cites demonstrates that a tamper resistant barrier may consist of software alone: Microsoft quotes from the '900 patent text that includes the following sentence: "No software-only tamper resistant barrier 674 can be wholly effective against all of these threats." (Microsoft's Markman Br. at 33 (quoting from '900 patent at 233:24–33) (emphasis added).) Obviously, the specification contemplates that a tamper resistant barrier may be software-only; such a software-only tamper resistant barrier, however, will not be wholly effective against all the threats identified. Had the inventors intended to exclude software-only mechanisms or processes from the definition of tamper resistant barrier, they would have said something to the effect of "no software-only mechanisms or processes can be a tamper resistant barrier because they cannot be wholly effective against all of these threats." Similarly, Microsoft's quotations of certain portions of specifications in support of its definition demonstrate only that a tamper resistant barrier may be a hardware device under the appropriate circumstances; but these quotations do not demonstrate that it must be a hardware device. (See, e.g., id. (quoting '193 patent at 49:15–17) ("A hardware SPU (rather than a software emulation) with a VDE node is necessary if a highly trusted environment for performing certain VDE activities is required."); see also id. at 32–34.) Finally, Microsoft's practice, utilized frequently in its discussion of other claim terms and phrases, of faulting InterTrust's proposed definition for not addressing certain questions, (id. at 34), is unconvincing because there is no evidence that it is even necessary to address these questions.

Accordingly, the Court adopts InterTrust's proposed definition and CONSTRUES "tamper resistant barrier" to mean: "Hardware and/or software that provides tamper resistance (defined supra)."

s. Use

InterTrust contends that the term "use" (193.19, 683.2, 721.1, 861.58, 891.1, 912.8, 912.35)

is not specially defined in the specification, and it is not a term of art. (InterTrust's Opening Markman Br. at 25.) InterTrust's proposed construction is based on the plain English meaning of the word use: "to put into service or apply for a purpose, to employ." (Id.) Microsoft's proposed construction appears similar, but it provides examples of the term use (e.g., copying, printing, decrypting) and requires an additional limitation pertaining to VDE. (See Microsoft's Markman Br. at 20–21.) Yet Microsoft does not clearly explain in its Markman brief how the first part of its proposed definition—"[t]o use information is to perform some action on it or with it"—is inconsistent with InterTrust's proposed definition, nor does it clearly explain the basis for the second part of its proposal, which imposes an additional limitation relating to VDE.

At oral argument the Court expressed its uncertainty regarding Microsoft's position in these two respects. Counsel for Microsoft informed the Court that it would be a "reasonable approach" for the Court to take if it struck out the second part of its proposed definition (the portion pertaining to VDE). (Tr. at 228:9–12.) As for the first part of its proposed definition, Microsoft's counsel stated that its proposed definition was intended only to provide examples of "use" for the jury to better understand the term in the sense Microsoft intended. (See Tr. 224:18–14, 227:8–228:8, 229:7–22.)

The Court discerns insufficient support for the second part of Microsoft's proposal, and in light of Microsoft's willingness to excise it, the Court agrees that this part is not due serious consideration. As for the first part of Microsoft's proposal, the Court believes that providing the examples of the term use that Microsoft has listed adds nothing in the way of clarification to the definition of the term and may in fact confuse the jury. Specifically, Microsoft does not indicate that these examples are exhaustive or that they have a particular relationship. Thus, a jury will be required to guess at their significance to determine what limiting purpose they serve, if any. At the same time, InterTrust's definition is more straightforward and is in fact consistent with this first portion of Microsoft's proposed definition.

Accordingly, the Court adopts InterTrust's proposed definition and CONSTRUES "use" to mean: "To put into service or apply for a purpose, to employ."

t. Virtual Distribution Environment (VDE)

InterTrust points out that among the twelve claims at issue in the mini-Markman proceeding, the term "virtual distribution environment" ("VDE") (900.155) appears only in the preamble of 900.155. (InterTrust's Opening Markman Br. at 35.) It argues that the individual elements of 900.155 fully define the recited apparatus, and reference to the preamble is not necessary to define and understand the claimed apparatus. (Id.) Citing Altiris, Inc. v. Symantec Corp., 318 F.3d 1363, 1371 (Fed. Cir. 2003), and Alfred J. Schumer v. Laboratory Computer Systems, Inc., 308 F.3d 1304, 1310 (Fed. Cir. 2002), InterTrust contends that the preamble does not "give life, meaning and vitality" to the claim, and therefore it is irrelevant to claim interpretation. (InterTrust's Opening Markman Br. at 35.) Accordingly, InterTrust asserts that VDE need not be defined and should not be read into claims that do not actually recite it. (See id.)

Without waiving its position that VDE should not be read into claims that do not actually recite it, InterTrust argues that to the extent it must be defined, the Court should adopt the short definition that it proposes, which is taken directly from embodiments of VDEs described in the specification. (Id.) InterTrust faults Microsoft's proposed definition, which consists of over 2,000 words, as incomprehensible by a lay jury. (Id.) It further criticizes Microsoft's proposed definition's requirement of a "secure processing environment" embodiment as conflicting with the specification's clear description of an alternate embodiment HPE. (Id.) It adds that, given that Microsoft seeks to read VDE into each and every claim, the "universe-wide" feature of VDE required in Microsoft's definition would appear impossible to apply to a claim relating to a single device or process. (Id. at 35–36.) It also insists that the requirements in Microsoft's definition that a VDE "guarantee" various types of security and that a VDE be "non-circumventable" is inconsistent with the real-word fact that guaranteed security is impossible, and it is inconsistent with the specification. (Id. at 36.)

Microsoft proposes a definition that is nothing short of gargantuan in length. Its proposed definition purports to be derived from numerous statements in the Big Book application. (See Microsoft's Markman Br. at 3–9.) Microsoft does not address InterTrust's contention that VDE should not be defined separately from the elements of 900.155 because it is found in the preamble and arguably does not give "life, meaning, or vitality" to the claim.

The Court agrees with InterTrust that VDE does not require construction independent of the elements of 900.155. The Court cannot possibly discern what "life, meaning, or vitality" VDE imbues in the claim. The claim terms speak for themselves. Moreover, the Court has difficulty accepting Microsoft's proposed definition of VDE to the extent it purports to be premised on the Big Book application where, as discussed supra, the PTO determined that the Big Book described five different inventions. Finally, given that the Court has stricken the Maier Declaration, the Court has no evidentiary basis to conclude that VDE would be construed by a person of ordinary skill in the art in the manner that Microsoft suggests. Accordingly, the Court adopts InterTrust's proposal and CONSTRUES "virtual distribution environment," as that term appears in 900.155, to be defined by the elements of 900.155; it has no definition independent of those elements.

IV. CONCLUSION

Despite its misgivings, the Court agreed to conduct this mini-Markman proceeding and resolve Microsoft's motion for summary judgment on indefiniteness at this stage of the litigation based on the parties' representations that early resolution of these matters would facilitate compromise. The Court also agreed to enter the partial stay of this action on Microsoft's request based on Microsoft's representations that proceeding with this litigation full-throttle might prove unnecessary if the Court would construe a key subset of claim terms and phrases and resolve certain other issues in dispute. To these ends the Court has expended tremendous time and effort.

Microsoft's decision to ignore approximately 40 percent of the claim terms and issues which were selected by the parties and its failure to provide substantial citations to evidentiary and legal authorities in support of its positions call into question the prudence of the Court's having proceeded in this fashion. It also lends credence to the suggestion that Microsoft's purported opposition to many of InterTrust's proposed constructions is baseless, and it implies that to a large extent the eight-month delay in this case has been for naught. It was Microsoft, after all, that proposed that thirty claim terms and phrases should be construed in this proceeding, arguing in a submission to the Court that construction of this many terms and phrases "should suffice to cover the most important disputes." That Microsoft evidently felt entitled to multiply the proceedings needlessly is more than a little disconcerting.

United States District Court
For the Northern District of California

The Court expects the parties now to conduct compromise negotiations earnestly and in good faith, as would be expected by their earlier representations to the Court. In the meantime, the Court wishes to make the following unequivocal: The Court will not tolerate a party's creating a dispute by taking a position on a material issue where that party does not have a good-faith basis for that position that is well-supported by fact and by law. Such conduct may result in the imposition of sanctions under Federal Rule of Civil Procedure 11 and/or other authority that may be applicable. Microsoft should be aware that this instruction applies with special force to it in light of its objectionable performance in the instant proceedings.

Accordingly,

IT IS HEREBY ORDERED THAT:

1. Microsoft's Motion for Summary Judgment that Certain "Mini-Markman" Claims Are Invalid for Indefiniteness [Docket No. 229] is DENIED.

2. Claims 193.1, 193.11, 193.15, 193.19, 683.2, 721.1, 721.34, 861.58, 891.1, 900.15, 912.8, and 912.35 are CONSTRUED as set forth in the body of this Order.

3. Consistent with the parties' representations to the Court in their joint letter dated June 26, 2003, and the Court's consideration thereof, **no later than July 9, 2003,** the parties shall file with the Court a joint statement of any reasonable length explaining whether the parties have obtained the consent of an Article III Judge of the Northern District of California to conduct settlement discussions (and if so, which Judge), and if not, what, if anything, the parties would like the Court to do to assist in their conducting settlement discussions. The Court will issue an appropriate Order shortly thereafter pertaining to such settlement proceedings.

4. The parties shall **telephonically** appear at a Case Management Conference before the Court on **August 7, 2003, at 3:~~15~~30 p.m.** InterTrust's counsel shall set up the **telephonic** conference call with all the parties on the line and call chambers at (510) 637-3559 at the time designated above. **NO PARTY SHALL CONTACT CHAMBERS DIRECTLY WITHOUT PRIOR AUTHORIZATION OF THE COURT.** The parties shall file a Joint Case Management Statement at least ten (10)

days prior to the conference.

IT IS SO ORDERED.

Dated: July 3, 2003

SAUNDRA BROWN ARMSTRONG
United States District Judge

United States District Court
For the Northern District of California